Číslo smlouvy NTK	194/2023
Číslo smlouvy Uživatel	

Smlouva o zajištění služeb ORCID

uzavřená podle § 1746 odst. 2 zákona č. 89/2012 Sb., občanský zákoník (dále jen "Smlouva"), jejímiž účastníky jsou

Národní technická knihovna, příspěvková organizace
se sídlem: Technická 6/2710, 160 80 Praha 6
zastoupená: Ing. Martinem Svobodou, ředitelem
IČO: 61387142
DIČ: CZ61387142
IDDS: syd69w9
(dále jen "NTK")

a

Vysoká škola báňská – Technická univerzita Ostrava
se sídlem: 17. listopadu 2172/15, 708 00 Ostrava-Poruba
zastoupená: prof. RNDr. Václav Snášel, CSc.
IČO: 61989100
DIČ: CZ61989100
IDDS: d3kj88v
(dále jen „Uživatel")

(všichni společně dále jen „Smluvní strany")

1. Preambule

Vzhledem k tomu, že

1.1. Společnost ORCID poskytuje služby, které umožňují transparentní a důvěryhodné spojení mezi výzkumnými pracovníky, jejich výsledky výzkumu a jejich afiliací, a to poskytováním jedinečného trvalého identifikátoru, který mohou jednotlivci používat v případě zapojení do výzkumných, studijních a inovačních aktivit, a

1.2. NTK považuje zprostředkování těchto služeb vysokoškolským institucím, neziskovým organizacím, výzkumným organizacím nebo výzkum financujícím agenturám se sídlem v České republice za součást plnění svých hlavních činností stanovených ve Zřizovací listině NTK,

dohodly se Smluvní strany tak, že NTK na základě oprávnění uděleného v této Smlouvě uzavře se společností ORCID „Smlouvu o vedení konsorcia", jejíž nedílnou přílohou jsou „Smluvní podmínky". Za podmínek a v souladu se „Smlouvou o vedení konsorcia" uzavírá NTK tuto Smlouvu, která zavazuje Smluvní strany dodržovat zde specifikované podmínky vzájemné spolupráce a partnerství mezi Smluvními stranami při užívání služeb společnosti ORCID. Služby budou zajišťovány prostřednictvím Národního centra ORCID.

2. Definice pojmů

2.1. Používá-li Smlouva v dalším textu termíny psané s velkým počátečním písmenem, ať už v singuláru nebo plurálu, mají tyto termíny následující význam:

2.1.1. **Modelem financování** se rozumí podíl a způsob úhrady Poplatků za Služby, přičemž NTK je oprávněna kdykoliv navrhnout změnu Modelu financování, a to ze závažných důvodů, zejména však z důvodu vyčerpání Zdroje financování, a postupovat, jak je dále specifikováno v čl. 7 Smlouvy;

2.1.2. **NTK** se rozumí Smluvní strana Smlouvy, jež zprostředkovává Služby a jiné Související služby Uživateli podle Smlouvy a Smlouvy o vedení konsorcia s cílem snížení nákladů na implementaci a využívání Služeb;

2.1.3. **Oprávněním API** se rozumí jedinečný přístupový kód, který společnost ORCID poskytuje každému Uživateli k používání Rozhraní API;

2.1.4. **Politikou Národního centra ORCID** se rozumí dokument dostupný na webu www.identifikatory.cz, který stanovuje informace o poskytování služeb, roli NTK a Uživatele a představuje rámec spolupráce mezi nimi;

2.1.5. **Poplatky** se rozumí poplatky za užívání Služeb, které jsou hrazeny v závislosti na Modelu financování a jejichž výše se odvíjí od počtu Uživatelů, kteří Služby v daném období využívají;

2.1.6. **Právem duševního vlastnictví** se rozumí zejména autorské právo, práva související s právem autorským, právo pořizovatele databáze a know-how;

2.1.7. **Přílohami** se rozumí Příloha A a B Smlouvy;

2.1.8. **Rozhraním API** se rozumí strojový přístup k registru ORCID prostřednictvím členského Oprávnění API;

2.1.9. **Službami** se rozumí licence k užívání členského Rozhraní API, které umožňuje strojový přístup k registru ORCID, jenž obsahuje jedinečné trvalé identifikátory a seznam aktivit k nim připojených;

2.1.10. **Smlouvou o vedení konsorcia** se rozumí smlouva mezi NTK a společností ORCID, jež tvoří společně se Smluvními podmínkami přílohu A Smlouvy;

2.1.11. **Smluvními podmínkami** se rozumí adhezní smluvní podmínky užívání Služeb, závazné pro NTK a Uživatele, které uzavírá NTK se společností ORCID, jež jsou nedílnou součástí Smlouvy o vedení konsorcia a jež tvoří společně se Smlouvou o vedení konsorcia přílohu A Smlouvy;

2.1.12. **Souvisejícími službami** se rozumí služby, které poskytuje NTK (Národní centrum ORCID) na základě Smluvních podmínek a které napomohou integraci služeb ORCID do systémů Uživatele, specifikované zejména na webové stránce: https://info.orcid.org/orcid-for-consortia/roles-and-responsiblities/;

2.1.13. **Společností ORCID** se rozumí nezisková organizace se sídlem 10411 Motor City Drive, Suite 750, Bethesda MD 20817, USA; registrovaná ve státě Delaware podle United States Code Title 26 - INTERNAL REVENUE CODE § 501(c)(3); poskytující na základě licenčního oprávnění Uživateli Služby;

2.1.14. **Standardními smluvními doložkami pro předávání údajů** se rozumí smluvní doložka závazná pro Společnost ORCID, jež zakotvuje, že Společnost ORCID zajistí úroveň ochrany osobních údajů odpovídající požadavkům evropských zákonů a předpisů na ochranu osobních údajů (Standard Contractual Clauses) a jež tvoří přílohu B Smlouvy;

2.1.15. **Uživatelem** se rozumí Smluvní strana Smlouvy, která je vysokoškolskou institucí nebo neziskovou organizací nebo výzkumnou organizací nebo výzkum financující agenturou se sídlem v České republice, zřízená podle zákonů České republiky a má zájem o čerpání Služeb na základě Smlouvy;

2.1.16. **Zdrojem financování** se rozumí projekt Czech Academic and Research Discovery Services (CARDS) realizovaný v letech 2023 až 2028, který realizuje NTK.

3. Předmět Smlouvy

3.1. Předmětem Smlouvy je:

3.1.1. závazek Uživatele zplnomocnit NTK k jednání se Společností ORCID;

3.1.2. závazek NTK:

a) na základě zplnomocnění Uživatele upraveném v čl. 4.1 Smlouvy jednat jménem Uživatele se Společností ORCID;

b) uzavřít se Společností ORCID dokumenty, jež tvoří Přílohy A a B Smlouvy;

c) zpřístupnit Uživateli Služby předáním požadovaných údajů o Uživateli Společnosti ORCID a uhrazením Poplatků ze Zdroje financování;
d) poskytovat Uživateli Související služby podle Smluvních podmínek; a
e) informovat a koordinovat Uživatele za účelem řádného čerpání služeb (dále specifikováno v čl. 4.4 Smlouvy, a

3.1.3. závazek Smluvních stran:
a) dodržovat Smlouvu, Přílohy a Politiku Národního centra ORCID; a
b) vzájemně spolupracovat a podílet se společně na aktivitách souvisejících se Službami.

4. Práva a povinnosti NTK při využívání Služeb

4.1. Uživatel tímto zplnomocňuje NTK k úkonům dle tohoto článku Smlouvy a souvisejícím úkonům, které jsou nutné pro poskytování Služeb dle této Smlouvy.

4.2. Smluvní strany tímto sjednávají, že NTK bezúplatně, na základě tohoto zplnomocnění Uživatele a jeho jménem zajistí uzavření:
a) Smlouvy o vedení konsorcia mezi NTK a Společností ORCID, jejíž součástí jsou Smluvní podmínky (ORCID Consortium Membershio Terms and Conditions) a odkazem začleněné ORCID Privacy Policy, ORCID Dispute Procedures a Member Benefits;
b) Standardních smluvních doložek pro předávání údajů.

4.3. NTK se zavazuje plnit závazky, které pro ni ze Smlouvy a Příloh plynou.

4.4. Smluvní strany tímto sjednávají, že NTK včas zajistí na základě zplnomocnění Uživatele uhrazení Poplatků ORCIDU v souladu se Smlouvou o vedení konsorcia.

4.5. NTK se zavazuje pravidelně informovat Uživatele o své činnosti související se Smlouvou, se Službami a Souvisejícími službami na pravidelných poradách nebo jiných schůzkách podle dohody Smluvních stran. NTK je povinna písemně oznámit Uživateli konání takové porady nebo jiné schůzky alespoň 14 dnů před konáním této porady nebo schůzky. NTK vezme v úvahu při plánování porad a schůzek časové možnosti Uživatele.

4.6. Veškerá komunikace Uživatele se Společností ORCID bude probíhat prostřednictvím NTK, která je povinna postupovat při zajišťování předmětu Smlouvy s odbornou péčí, pracovat na profesionální úrovni a chránit zájmy Uživatele.

4.7. Hlavní kontaktní údaj ke službám ORCID na straně NTK je e-mailová adresa: **orcid@techlib.cz.**

5. Práva a povinnosti Uživatele při využívání Služeb

5.1. Služby může Uživatel čerpat nejdříve od 1. června roku uzavření Smlouvy.

5.2. Uživatel potvrzuje, že se s obsahem Příloh Smlouvy detailně seznámil a zavazuje se plnit závazky, které pro něj z Příloh Smlouvy plynou, a k dodržování Příloh této Smlouvy zaváže i všechny své zaměstnance a kontraktory při činnosti související se Službami a Souvisejícími službami.

5.3. Uživatel je povinen předat včas NTK veškeré podklady, dokumenty a informace, jež jsou potřebné ke splnění Smlouvy. Současně se zavazuje s NTK spolupracovat.

5.4. Uživatel tímto uděluje souhlas s použitím svého oficiálního názvu a loga na webových stránkách Společnosti ORCID orcid.org zejména pro účely prezentace poskytování služeb ORCID.

5.5. Uživatel tímto uděluje souhlas s použitím svého oficiálního názvu a loga na webových stránkách NTK, jimiž jsou orcid-cz.org a identifikatory.cz, zejména pro účely prezentace zprostředkování Služeb.

5.6. Strany se zavazují vyvinout veškeré úsilí k efektivnímu využívání Služeb, zejména účastnit se schůzek, které organizuje NTK, a efektivně implementovat Služby ve své instituci.

5.7. Uživatel zajistí kontaktní osobu pro administrativu a kontaktní osobu pro technické záležitosti a zavazuje se při uzavření Smlouvy předat NTK kontaktní údaje pověřených osob na e-mailovou adresu: **orcid@techlib.cz.** Uživatel odpovídá za aktuálnost kontaktních údajů pověřených osob a souhlasí se zveřejněním těchto údajů na webu orcid-cz.org a identifikatory.cz.

5.8. Uživatel je povinen oznámit bez zbytečného odkladu jakékoli změny v kontaktních údajích na e-mailovou adresu: **orcid@techlib.cz.**

5.9. Uživatel se zavazuje poskytnout NTK potřebnou součinnost při kontrolách, kterým podléhá NTK ze zákona nebo podle pravidel souvisejících s financováním (operační program Jan Amos Komenský), a případně se sám podrobit této kontrole ze strany kontrolních orgánů v souvislosti s plněním Smlouvy.

6. Práva duševního vlastnictví

6.1. Smluvní strany se dohodly na tom, že jakýkoliv předmět Práva duševního vlastnictví vzniklý v rámci poskytování Služeb a Souvisejících služeb bude ve vlastnictví té Smluvní strany, která ho vytvořila jako zaměstnanecké dílo podle zákona č. 121/2000 Sb. o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (dále jen „autorský zákon a pomocí vlastních materiálních a finančních vkladů, a to bez finančního nebo personálního přispění další Smluvní strany.

6.2. Smluvní strany se dále zavazují zveřejnit výsledky vzniklé v rámci poskytování a využívání Služeb pod licencí CC BY 4.0 Mezinárodní[1] nebo po dohodě Smluvních stran pod jinou licencí Creative Commons, pokud tomu nebrání práva třetích stran nebo závazná pravidla financování Služeb. Zveřejňování výsledků se řídí zásadou „As Open as Possible, As Closed as Necessary".

6.3. Vznikne-li nový předmět Práva duševního vlastnictví za přispění více Smluvních stran, je takový předmět Práva duševního vlastnictví ve spoluvlastnictví více Smluvních stran. Poměr podílů se odvíjí od výše podílu na činnostech při vzniku předmětu Práva duševního vlastnictví. U autorských děl se tento odstavec použije obdobně na výkon majetkových práv k autorskému dílu.

6.4. Uživatel tímto souhlasí s ukládáním a zveřejňováním jakýchkoliv metodických materiálů zabývajících se užíváním Služeb, pokud jsou zaměstnaneckými díly Uživatele podle autorského zákona, a to v institucionálním repozitáři NTK, na webových stránkách NTK, jimiž jsou orcid-cz.org a identifikatory.cz a případně na dalších kanálech na základě domluvy Uživatele a NTK.

7. Model financování služeb

7.1. Poplatky za poskytování Služeb jsou v plné výši financovány prostřednictvím NTK ze Zdroje financování.

7.2. Model financování je NTK oprávněna jednostranně změnit ze závažných důvodů, zejména však z důvodu vyčerpání Zdroje financování, a to s platností k datu nejbližšího automatického obnovení smlouvy dle čl. 8.1. Smlouvy. NTK bude Uživatele informovat o změně Modelu financování nejméně 120 dní před datem nejbližšího automatického obnovení Smlouvy.

7.3. Související služby jsou Uživatelům poskytovány bezplatně.

7.4. Strany se zavazují, v případě změny Modelu financování podle čl. 7.2, upravit výslednou změnu dodatkem ke Smlouvě nebo vypovědět Smlouvu podle čl. 8.3 nebo 8.5 Smlouvy a plnit všechny případné povinnosti, které v souvislosti se změnou Modelu financování mohou vzniknout, zejména hrazení Poplatků ze strany Uživatele na základě upraveného Modelu financování.

7.5. NTK je výhradně odpovědná za řádné čerpání Zdroje financování.

8. Trvání smlouvy

8.1. Smlouva se uzavírá ode dne podpisu všemi Smluvními stranami do 31. května následujícího roku a automaticky se obnovuje vždy na období jednoho roku od 1. června daného roku, pokud kdykoliv v průběhu roku, nejpozději však 90 dnů před tímto datem nepodal Uživatel výpověď ze Smlouvy. Výpověď je nutné podat NTK doporučené poštou nebo prostřednictvím datové schránky a její účinky nastávají k datu nejbližšího automatického obnovení Smlouvy.

8.2. Pokud Společnost ORCID upraví znění Smluvních podmínek uzavřených s NTK v souladu s ustanoveními oddílu 8.2 Smluvních podmínek (Příloha A), NTK oznámí Uživateli změny do 14 dnů od obdržení oznámení o změně. Pokud Uživatel vznese námitky proti jakýmkoli takovým úpravám, je Uživatel oprávněn vypovědět Smlouvu do 30 dnů od doručení takového oznámení s účinností ke dni účinnosti upravených Smluvních podmínek. Výpověď musí být doručena doporučené poštou nebo prostřednictvím datové schránky.

8.3. Pokud NTK změní Politiku Národního centra ORCID nebo Model financování, NTK oznámí Uživateli změny nejpozději 120 dní před datem nejbližšího automatického obnovení Smlouvy. Každý Uživatel je oprávněn vypovědět Smlouvu do 30 dnů od oznámení od NTK o změně Politiky Národního centra ORCID nebo Modelu financování, a to doporučené poštou nebo prostřednictvím datové schránky, s účinností ke dni nejbližšího automatického obnovení Smlouvy.

---

[1] CC BY 4.0 Mezinárodní se rozumí veřejná licence Creative Commons, jejíž text je dostupný na https://creativecommons.org/licenses/by/4.0/legalcode.cs

8.4. NTK je oprávněna vypovědět s účinností ke dni nejbližšího automatického obnovení Smlouvy (neprodloužit) Smlouvu v případě ukončení Smlouvy o vedení konsorcia mezi NTK a Společností ORCID podle čl. 7.2 nebo čl. 7.3 Smluvních podmínek (Příloha A).

8.5. NTK je oprávněna vypovědět s účinností ke dni nejbližšího automatického obnovení Smlouvy (neprodloužit) Smlouvu, pokud Uživatel Smlouvu poruší. Porušením Smlouvy se rozumí zejména:

a) porušení Smluvních podmínek (Příloha A);

b) neuzavření dodatku v případě změny Modelu financování a zároveň nevypovězení Smlouvy podle odst. 3 tohoto článku Smlouvy.

8.6. V případě výpovědi nebo neprodloužení Smlouvy podle odst. 4 a odst. 5 tohoto článku Smlouvy zašle NTK Uživateli oznámení o ukončení Smlouvy.

8.7. Oznámením dle tohoto článku se rozumí písemná zpráva, která byla prokazatelně doručena druhé Smluvní straně.

9. Závěrečná ustanovení

9.1. Uživatelem se může stát pouze vysokoškolská instituce, nezisková organizace, výzkumná organizace nebo výzkum financující agentura se sídlem v České republice, zřízená podle zákonů České republiky.

9.2. Žádný projev Smluvních stran učiněný při jednání o Smlouvě ani projev učiněný po uzavření Smlouvy nesmí být vykládán v rozporu s výslovnými ustanoveními Smlouvy a nezakládá žádný závazek žádné ze Smluvních stran. Smluvní strany si nepřejí, aby nad rámec výslovných ustanovení Smlouvy byla jakákoliv práva a povinnosti dovozovány z dosavadní či budoucí praxe zavedeně mezi Smluvními stranami či zvyklostí zachovávaných obecné či v odvětví týkajícím se předmětu plnění Smlouvy, ledaže je ve Smlouvě výslovně sjednáno jinak.

9.3. Každá ze Smluvních stran je povinna se zdržet jakékoliv činnosti, jež by mohla znemožnit nebo ztížit dosažení účelu Smlouvy. Dále je každá ze Smluvních stran povinna se zdržet jakéhokoliv jednání, které by mohlo ohrozit zájmy druhé Smluvní strany v souvislosti s dosažením účelu Smlouvy.

9.4. Smlouva se řídí českým právem a české soudy jsou příslušné k rozhodování veškerých případných sporů vzniklých z této Smlouvy.

9.5. Změny nebo doplňky Smlouvy lze provést pouze ve formě písemných, vzestupně číslovaných dodatků. Za písemnou formu se pro účely této Smlouvy považuje listinná i elektronická forma.

9.6. Smluvní strany bezvýhradně souhlasí se zveřejněním plného znění Smlouvy tak, aby Smlouva mohla být předmětem poskytnuté informace ve smyslu zákona o svobodném přístupu k informacím ve znění pozdějších předpisů, a zákona o registru smluv ve znění pozdějších předpisů.

9.7. Tato smlouva nabývá platnosti dnem podpisu oprávněnými zástupci smluvních stran a účinnosti dnem zveřejnění v registru smluv. NTK se zavazuje, že provede zveřejnění této Smlouvy v registru smluv, a to bez zbytečného odkladu, nejpozději však do 30 dnů od uzavření této Smlouvy.

9.8. Nedílnou součást Smlouvy jako její samostatné přílohy jsou:
Příloha A – Smlouva o vedení konsorcia (v originále: Consortium Lead Agreement) a Smluvní podmínky (ORCID Consortium Membership Terms and Conditions)
Příloha B – Standardní smluvní doložky (v originále Standard Contractual Clauses for the Transfer of Personal Data to Third Countries)

V Praze dne	V dne
za NTK	za Uživatele

[redacted]

10. Příloha A – Smlouva o vedeni konsorcia (v originále: Consortium Lead Agreement) a Smluvní podmínky (ORCID Consortium Membership Terms and Conditions)

Příloha A obsahuje původní znění Smlouvy o vedení konsorcia v anglickém jazyce a následně i překlad do češtiny.

ORCID Consortium Agreement

Consortium Lead Agreement

Consortium Lead: The National Library of Technology
Entity Type: State Contribution Organization set up by the Ministry of Education, Youth and Sports in the Czech Republic
Location: Technická 2710/6, 160 80 Praha, Czech Republic
iD No.: CZ61387142

This Consortium Lead Agreement is entered into by and between ORCiD, inc., a Delaware nonstock corporation located at 10411 Motor City Drive, Suite 750, Bethesda, MD 20817, USA ("ORCID"), and Consortium Lead, as of the Consortium Effective Date (as defined below). In consideration of the mutual promises contained herein and for other good and valuable consideration, the receipt and sufficiency of which are acknowledged, ORCiD and Consortium Lead hereby agree to the terms, conditions and obligations set forth below and in Exhibit 1 and the ORCiD Consortium Membership Terms and Conditions ('Terms and Conditions"), each of which is attached hereto and incorporated herein by reference.
Capitalized terms not defined elsewhere are defined in Article 9 of Terms and Conditions.

	Consortium Lead **Main Contact**	**Consortium Lead** **Administrative Contact**	**Consortium Lead** **Technical Contact**
Name:			
Title:			
Address:			
Email:			
Telephone:			

ORCiD Main Contact:

ivo Wijnbergen, Director of Engagement, ORCiD, inc., 10411 Motor City Drive, Suite 750, Bethesda, MD 20817, USA; membership@orcid.org; [redacted]

initial Term: 01/06/2023 ("Consortium Effective Date") through 31/05/2024, subject to termination and renewal as set forth in the Terms and Conditions.

Consortium Members: As further described on Exhibit 1 (attached hereto and incorporated herein by reference), Consortium Lead shall maintain a list through the ORCiD self-service tool at http://orcid.org/self-service (as updated from time to time, the "Consortium Member List") of entities (each, a "Consortium Member" and collectively, the "Consortium Members"), including Consortium Lead if relevant, that are to be Members of ORCiD and entitled to the Member Benefits, as defined on the ORCiD website (https://info.orcid.org/membership). Consortium Lead shall complete the Consortium Member List of initial Consortium Members prior to the Consortium Effective Date. Thereafter, Consortium Lead may update the Consortium Member List from time to time. Each proposed entity shall become a Consortium Member upon acceptance by ORCiD.

Consortium Lead represents and warrants that it has all necessary power and authority to (i) enter into to this Consortium Lead Agreement and the Terms and Conditions on its own behalf, (ii) act as agent and bind each Consortium Member set forth on the Consortium Member List to the Terms and Conditions, and that by signing this Consortium Lead Agreement, the Terms and Conditions shall be legally binding upon Consortium Lead and each Consortium Member listed on the Consortium Member List.

Only institutions of higher education, nonprofit organizations, and government research and funding agencies located in and organized under the laws of the Czech Republic are entitled to be covered under the Consortium Fee (defined below),

and Consortium Lead represents and warrants that each institution listed on the Consortium Member List is such an entity.

Consortium Fee:

ORCID Classification: Consortium

Initial Consortium Composition: (*# of members per tier; to be completed by ORCID*)

Initial Consortium Fee: (*to be completed by ORCID*)

Consortium Lead shall be responsible for collecting and paying an annual membership fee (the "Consortium Fee") to ORCID set forth in the fee schedule on the ORCID website at https://info.orcid.org/membership **according to the number of Consortium Members and the fee tier of each member (the "Consortium Composition").**

The Consortium Fee shall be due net 45 days from signing this Consortium Lead Agreement. If Consortium Lead adds any additional Consortium Members during the Initial Term or a Renewal Term resulting in an increase in the Consortium Composition set forth above, ORCID will charge additional fees on a pro-rated basis which shall be due net 45 days from the date such changes take place.

Renewal fees shall be due net 45 days from the date set forth in an annual invoice sent by ORCID. Lower or higher fees based on the Consortium Composition will be evaluated at each Renewal Term.

All payments shall be made in United States Dollars. Any undisputed payments made more than sixty (60) days after they are due and payable shall be subject to a 1.5% monthly interest charge, and ORCID reserves the right to freeze access to Consortium Members' API Credentials until undisputed payments are made. All payments shall be made by mutually acceptable form of wire transfer to ORCID, by credit card, or check payable to ORCID Inc.

Consortium Fees exclude any applicable taxes. If the Consortium Fee is subject to any taxation (other than income taxation to ORCID in the United States), then the Consortium Lead shall be responsible for (i) the cost of such tax and (ii) outside the United States, remitting such tax wherever legally permissible.

ORCID reserves the right to charge additional fees for any additional Member Benefits that become available and that Consortium Lead elects to license on behalf of the Consortium Members during the Initial Term or a Renewal Term. If at any time during the Term or a Renewal Term there are fewer than 5 Consortium Members, the fees will be adjusted to ORCID's standard direct membership fees and the discount rate shall no longer apply effective immediately. Annual fee increases generally will be no more than 3% per annum (not taking into account changes in the Consortium Composition or rounding of per-member fees), and ORCID will provide no less than 60 days' advance notice to Consortium Lead of any such fee increase. ORCID reserves the right to restructure the consortium fee model from time to time at its discretion, and if such changes result in an in increase in the Consortium Fee of more than 3% other than due to changes in the Consortium Composition, ORCID will provide no less than 12 months' advance note of any such change. Notwithstanding Section 6.2 of the Terms and Conditions, Consortium Lead will be liable for all actual, direct and reasonable costs and expenses (including without limitation, reasonable attorneys' fees) incurred by ORCID in collecting any past due amounts.

Use of Trademark: ORCID is a community-based initiative and as such, is eager to promote the participation of its Members. To that end, if the "Agree" box is checked below, ORCID may use during the Initial Term and any Renewal Term Consortium Lead's name and logos for the limited purposes of indicating that ORCID and Consortium Lead have entered into this Consortium Lead Agreement, and to publicize any links Consortium Lead creates from its website to the ORCID website.

☐ Agree

Consortium Lead is encouraged to use ORCID's name, logo, and other trademarks (the "Marks") to announce the ORCID Consortium and its status as the Consortium Lead, provided that it correctly identifies the Marks as a trademark under US and other laws if requested by ORCID. (See ORCID Brand Guidelines.) Consortium Lead may not use the Marks in any way likely to cause confusion as to the origin of goods or services or to suggest endorsement by ORCID, except as specifically approved by ORCID in writing.

Support:

The Consortium Fee covers the provision of Member API Credentials for each Consortium Member set forth on the Consortium Member List plus the ORCID support set forth in the Roles and Responsibilities of ORCID Consortia (available at https://info.orcid.org/orcid-for-consortia/roles-and-responsiblities) . The Consortium Lead acknowledges (i) the roles and responsibilities of Consortium Lead set forth in Roles and Responsibilities of ORCID Consortia and agrees to implement the relevant support and services (including, without limitation, the technical support to be provided by Consortium Lead) within 90 days of the Consortium Effective Date; and (ii) the Consortium Fee is based on the Consortium Lead providing such services and failure to provide such services could result in an increase in the Consortium Fee.

Notices:
Any notice required to be given by ORCID under the Terms and Conditions shall be given only to Consortium Lead's Main Contact. It is Consortium Lead's responsibility to keep its contact information up to date and to forward any such notice to the Consortium Members in a timely manner.

Miscellaneous: Sections 8.3 through 8.10 of the Terms and Conditions shall apply equally to the construction, interpretation and enforcement of this Consortium Lead Agreement as part of the Consortium Agreement. In the event of a direct conflict, this Consortium Lead Agreement shall govern over the Terms and Conditions.

This Consortium Lead Agreement and any amendments may be executed in one or more counterparts, each of which shall be deemed an original, but all of which shall constitute one agreement. **EACH PARTY MAY USE A PAPER (WET) OR ELECTRONIC SIGNATURE, EACH OF WHICH SHALL BE DEEMED TO BE AUTHENTIC AND EQUALLY ENFORCEABLE.**

This Agreement is drawn up in duplicate in Czech and English language for each of the Parties, both copies being authentic. In case of any divergence in the interpretation of this Agreement, the English version shall prevail.

IN WITNESS WHEREOF, ORCID and Consortium Lead have caused this Consortium Lead Agreement to be executed by a duly authorized representative, thereby entering into the Consortium Agreement.

The **National Library of Technology**	**ORCID,** Inc.
Signature:	Signature:
Name:	Name: Chris Shillum
Title:	Title: Executive Director
Email address:	Email address: [redacted]
Date:	Date:

Exhibit 1 to the Consortium Lead Agreement: Consortium Members

Consortium Lead shall maintain the Consortium Member List through the ORCID self-service tool at http://orcid.org/self-service, including the information listed below. Consortium Lead should include its name as well if it is becoming an ORCID Member. Consortium Lead is responsible for ensuring that the Consortium Member List remains up to date and accurate.

- **Organization Name**
- **Main Contact: Name, Job Title, Email.** The Main Contact indicated for each Consortium Member shall be the person who represents the Consortium Member for purposes of (i) notice under the Terms and Conditions and ORCID's bylaws and (ii) membership voting, and who otherwise acts on behalf of the Consortium Member under the Terms and Conditions and under ORCID's bylaws.
- **Technical Contact: Name, Job Title, Email.** The Technical Contact shall be the person responsible for managing the Member's API Credential(s).

In addition, Consortium Lead shall maintain a shared separate document at the following address www.identifikatory.cz with the following information:

- **Organization Name**
- **Organization Address**
- **Trademark License:** Indicate "Yes" if ORCID may use during the Initial Term and any Renewal Term the relevant Consortium Member's name and logos for the limited purposes of indicating that Consortium Member is a Member of ORCID and to publicize any links Consortium Member creates from its website to the ORCID website. Indicate "**No**" if such a license is not granted.

ORCID Consortium Membership Terms and Conditions

Consortium Lead: National Library of Technology

ORCID, Consortium Lead and each entity ("Consortium Member") set forth on the Consortium Member List as described in Exhibit **1** to the ORCID Consortium Lead Agreement signed by Consortium Lead and effective as of Consortium Effective Date is bound by the terms and conditions of these ORCID Consortium Membership Terms and Conditions ("Terms and Conditions") which incorporates by reference the ORCID Privacy Policy, ORCID Dispute Procedures, and the Member Benefits.

1. Grant of License from ORCID and Member Benefits. Each Consortium Member shall have the Member Benefits available to ORCID premium members which shall include at a minimum those benefits set forth in this Article **1**. Member Benefits may be added and amended from time to time by ORCID beyond those set forth in this Article 1, and current Member Benefits shall appear on the ORCID website. All Member Benefits are subject to the terms and conditions of these Terms and Conditions. The license set forth in Section **1.1** and the other Member Benefits shall remain in effect for the Initial Term (or relevant Renewal Term) set forth in the Consortium Lead Agreement (or a renewal notice), unless earlier terminated under Article 7, or restricted under Section 4.2.

1.1 Grant of License. As of the Effective Date, and subject to timely payment in full by Consortium Lead of the fees set forth in the Consortium Lead Agreement, ORCID grants to each Consortium Member a non-transferable license to use a Member API Credential(s) to access the Member APIs, and read, deposit/edit and Use Record Data subject to the relevant Privacy Settings and these Terms and Conditions. All rights not expressly granted herein are reserved by ORCID. Nothing herein shall require any Consortium Member to exercise any of the Member Benefits.

1.2 Consortium Members that are Service Providers. As used herein, "Service Provider" means an organization that provides services or products to other organizations based on the use of its Member API Credential(s), other Member Benefits, or the creation or authentication of ORCID Identifiers. Service Providers must require their customers to make use of their own API credentials, whether in the form of a free Public API Credential or a paid Member API Credential. ORCID reserves the right to determine if an application requires a separate API Credential; therefore, Service Providers are encouraged to discuss their plans with ORCID in advance of implementation.

1.3 Deposit/Edit Data. Each Consortium Member shall have the ability to deposit and edit Record Data in existing ORCID Records where the relevant Individual has granted the Consortium Member authority as a Trusted Organization, subject to the following:

(i) Each Consortium Member shall only deposit/edit the type and scope of Record Data for which it has consent from an Individual through the ORCID mechanism for granting consent to Trusted Organizations.

(ii) Each Consortium Member shall only deposit/edit Record Data that, to the best of its knowledge at the time of deposit/edit, is true and correct and is associated with the correct Individual and ORCID Identifier. If, after the time of deposit/edit, a Consortium Member becomes aware that any Record Data it deposited/edited is incorrect, the Consortium Member shall correct or inform the relevant Individual and ORCID. A Consortium Member is under no obligation to update Record Data other than to correct any Record Data that were not true and correct at the time of deposit/edit or inform ORCID and the relevant Individual that such Record Data is incorrect, and shall have no liability for ORCID's continued Use of uncorrected Record Data after the Consortium Member has corrected it or informed the relevant Individual and ORCID.

(iii) If a Consortium Member deposits/edits any links to articles, blogs, data sets or other works which may be subject to intellectual property protection, it shall only do so in a manner that does not to its knowledge violate the copyright or any other intellectual property rights of a third party.

(iv) Subject to these Terms and Conditions, each Consortium Member grants to ORCID a fully-paid, royalty-free, non-exclusive, worldwide, perpetual, irrevocable license for any and all rights necessary to allow ORCID and the public to Use such deposited/edited Record Data, subject to any Privacy Settings.

1.4 Data Searching, Downloads and Alerts. Each Consortium Member shall have access to the Member APIs to query the ORCID Registry and download Record Data, including Limited Access Data if granted the right by the relevant Individual or Trusted Individual. In addition, each Consortium Member shall have access to a mechanism for periodically synchronizing changes in the Public Data File.

1.5 Technical Support. ORCID will provide Consortium Lead and the Consortium Members with the technical support set forth in *the Roles and Responsibilities of ORCID Consortia* (available at https://info.orcid.org/orcid-for-consortia/roles-and-responsiblities/). Technical support must be coordinated through the Technical Contact set forth in the ORCID Consortium Lead Agreement and in the *Roles and Responsibilities* statement.

1.6 Privacy Enforcement. If a Consortium Member both mandates the use of ORCID identifiers and facilitates their collection using the ORCID APIs, the Consortium Member shall have the right, but not the obligation, to enforce on behalf of any Individual who it has mandated to use an ORCID Identifier ORCID's privacy commitments to the Individual as set forth in the ORCID Privacy Policy.

1.7 Nominations for ORCID Board & Participation in Governance Matters. Individuals representing each Consortium Member may exercise a Consortium Member's voting rights and be nominated to serve on the ORCID Board of Directors, consistent with ORCID's Bylaws which are available on the ORCID website. The person indicated by Consortium Lead as the Main Contact on the Consortium Member List for each Consortium Member shall be the person who represents the Consortium Member for purposes of notice, membership voting and otherwise exercising the Consortium Member's rights as a member under ORCID's Bylaws. (Consortium Member may change the name of the Main Contact through the Consortium Lead's support desk.)

1.8 Limitations on Consortium Member's Use. Each Consortium Member is prohibited from and agrees to the following restrictions:

(i) Not to allow any other entity to use its Member API Credential(s) except to assist that Consortium Member on the Consortium Member's own behalf;

(ii) Not to disclose to any other person or entity Limited Access Data unless (a) such data is publicly available from another source, or (b) the Consortium Member provides notice to the Individual how and to whom such data will be disclosed;

(iii) Not to deposit/edit types of data other than those permitted by a specified field, and not to include any full works in such fields (in other words, only metadata and links to works may be deposited and not texts of articles, blogs, or publications and datasets);

(iv) Not to deposit, edit, or modify any ORCID Record in a manner that knowingly makes it false, untrue, misleading or libelous in whole or in part, or knowingly make use of any ORCID Record in any manner that does any of the foregoing or violates the rights of publicity or privacy of any individual;

(v) Not to Use any Record Data to contact any Individual for marketing purposes without giving the Individual the right to opt-out of such marketing communications;

(vi) Not to use Record Data to send "junk mail," "spam," "chain letters," "pyramid schemes," or similar schemes;

(vii) Not to use Record Data to harass, abuse or harm another person;

(viii) Not to override, circumvent, or disable any encryption features or software protections employed to protect the security of the Member API Credential(s), the ORCID Registry or Record Data;

(ix) Not to manipulate ORCID identifiers to disguise the origin of any Record Data; knowingly upload or post any Record Data that contains software viruses or any other computer code, files, or programs designed to interrupt, destroy, or limit the functionality of any software, hardware, or telecommunications equipment; or intentionally interfere with or disrupt ORCID servers or networks;

(x) Not to use any or all of the Member API Credential(s) or its Member Benefits to create a service or product that allows organizations to obtain the benefits of those Member Benefits without being an ORCID Member; and

(xi) Not to use any or all of the Member API Credential(s), the Member Benefits, the Member APIs, or the ORCID Registry in violation of these Terms and Conditions, or in any manner that is otherwise illegal in the United States of America ("U.S.") and the jurisdiction in which the Consortium Member is located, if other than the U.S.

1.9 Limitations on ORCID's Use. ORCID shall only use and make available Record Data via the ORCID Registry and the Public Data File as permitted by these Terms and Conditions, and to the extent that any Record Data is edited or removed as permitted by these Terms and Conditions, the viewable ORCID Registry and future Public Data Files shall reflect such changes.

2. Intellectual **Property Ownership.**

2.1 Ownership of ORCID Registry and Marks. As between the parties, ORCID owns all rights, title, and interest, including without limitation, applicable database rights, in and to the ORCID Registry and the software developed by ORCID, the System Data, the Member APIs, the Member API Credential(s), and the ORCID Marks, as defined in Section 2.2 (collectively, the "ORCID Intellectual Property"); provided, however, ORCID Intellectual Property does not include any individual data elements in the ORCID Registry. ORCID makes its Registry software available under an open

source license whenever legally possible. (See Open Source Project on the ORCID website.)

2.2 Use of ORCID Trademarks. Consortium Member is encouraged to use ORCID's name, logo, and other trademarks (the "Marks") to announce its use of the ORCID Registry and status as a member of ORCID, provided that Consortium Member correctly identifies the Marks as a trademark under US and other laws if requested by ORCID. (See ORCID Brand Guidelines on the ORCID website.) Consortium Member may not use the Marks in any way likely to cause confusion as to the origin of goods or services or to suggest endorsement by ORCID, except as specifically approved by ORCID in writing.

3. Delivery and General Support.

3.1 Unavailability of the ORCID Registry. ORCID shall use commercially reasonable efforts to provide continuous availability of the ORCID Registry and the Member Benefits. However, Consortium Lead and each Consortium Member recognize that the ORCID Registry and the Member Benefits may not be available from time to time due to maintenance of the server(s), the installation or testing of software, and downtime relating to equipment or services outside the control of ORCID including, but not limited to, telecommunications services or Internet nodes or facilities; provided, however, that ORCID shall give Consortium Lead reasonable advance notice of any downtime within ORCID's reasonable control.

3.2 Premium Members. In addition to the other commitments set forth in these Terms and Conditions, ORCID shall provide Consortium Member a call-back API, higher allowed API requests per day, and custom reports and data files. Premium benefits also include the ability for each Consortium Member to be issued up to five (**5**) Member API Credentials for use in different system integrations at the same organization.

4. Privacy, Security and Usage Data.

4.1 Data Protection. ORCID shall use commercially reasonable efforts to protect the security and integrity of the ORCID Registry (including, without limitation, Member API Credentials, passwords, usernames, and IP addresses) and Record Data, as set forth in its Privacy Policy, including storing information in a data center with restricted access and monitoring, using secure socket and intrusion detection software, and hashing for passwords. ORCID shall promptly notify Consortium Lead upon learning of any material security breach related to a Consortium Member's API Credentials or upon ORCID's determination that there has been a material breach of the security of the ORCID Registry generally.

4.2 Protection of the Member API Credentials, the ORCID Registry and ORCID Record Data. Each Consortium Member agrees to use its Member API Credential(s) only as set forth in these Terms and Conditions and shall take reasonable efforts to protect its Member API Credential(s) from any security breaches or other use that is in violation of these Terms and Conditions or applicable law. Consortium Lead shall be liable for its intentional misconduct or negligent use of the Member API Credentials, except in the event that it establishes that a security violation is due to ORCID's fault. Each Consortium Member shall be liable for its intentional misconduct or negligent use of its Member API Credential(s), except in the event that it establishes that a security violation of its Member API Credential(s) is due to ORCID's fault. Consortium Lead and each Consortium Member shall notify ORCID promptly upon (i) learning of any violation or alleged violation of these Membership Terms and Conditions or security of a Member API Credential or the ORCID Registry or (ii) becoming aware that any Record Data the Consortium Member has deposited/edited violates or may violate the rights of privacy, publicity or other rights of an Individual. Furthermore, Consortium Lead and each Consortium Member shall cooperate fully with ORCID in investigating and curing violations or alleged violations, including, without limitation, assisting ORCID in providing Individuals with any required notices. Additionally, ORCID may (without limiting any other remedies ORCID may have) impose temporary restrictions on use of Member API Credentials and access to the ORCID Registry until the violation is cured.

4.3 Monitoring and Gathering Usage Data. To protect the security of Member API Credentials and the ORCID Registry against unauthorized uses and to learn about the uses made of the ORCID Registry and the Member APIs, ORCID may monitor activity and use of Member API Credentials and the Member APIs.

5. Disputed Data; Withdrawal of Data from the ORCID Registry. ORCID shall assist in resolving disputes between users (including, without limitation, between Individuals, Consortium Members, and other members) of the ORCID Registry regarding ORCID Identifier ownership claims, data accuracy and integrity, and Individual identity, in accordance with policies and procedures set forth in the ORCID Dispute Procedures, which is incorporated herein by reference. Notwithstanding the foregoing, ORCID makes no representation or warranty about, and shall not be responsible for the accuracy of data deposited in the ORCID Registry. ORCID reserves the right to remove from the ORCID Registry and its servers any Record Data or disable access to parts of the ORCID Registry as it deems necessary.

6. General Representations and Warranties, Disclaimers, Limitation of Liability. Each of ORCID and Consortium Lead represents and warrants that it has the authority to enter into the Consortium Lead Agreement and these Terms and Conditions, and to bind its organization to the terms and conditions of the Consortium Lead Agreement, including without limitation these Terms and Conditions. Each of ORCID and Consortium Lead further represents and warrants that it has caused the Consortium Lead Agreement to be executed by a duly authorized representative. Consortium Lead further represents and warrants that it has the authority to act on behalf of and legally represent and bind each Consortium Member listed on the Consortium Member List to these Terms and Conditions, and that, by executing the Consortium Lead Agreement, it has done so. Except as set forth herein, ORCID makes no representations or warranties regarding (a) the accuracy of Record Data; (b) misuse of Record Data by third parties; (c) freedom from defamation or infringement of rights of privacy though use of the Record Data; (d) lack of viruses, bugs or other impairments to computer systems and software; and (e) links to other websites and content found therein.

6.1 Disclaimer. OTHER THAN THE EXPRESS REPRESENTATIONS AND WARRANTIES STATED IN THESE TERMS AND CONDITIONS, THE ORCID REGISTRY, RECORD DATA, THE PUBLIC DATA FILE, THE MEMBER API CREDENTIAL(S), THE MEMBER APIs, AND/OR THE MEMBER BENEFITS (individually and collectively, the "ORCID SYSTEM") ARE PROVIDED ON AN "AS IS" BASIS, AND ORCID AND ITS DIRECTORS, OFFICERS, EMPLOYEES, AGENTS, CONTRACTORS, AND REPRESENTATIVES (individually and collectively, the "ORCID PARTIES") DISCLAIM TO THE FULLEST EXTENT PERMITTED BY LAW ANY AND ALL OTHER REPRESENTATIONS AND WARRANTIES OF ANY KIND (EXPRESS, IMPLIED, ORAL, OR WRITTEN) RELATING TO THE ORCID SYSTEM, INCLUDING, WITHOUT LIMITATION, ANY AND ALL IMPLIED WARRANTIES OF QUALITY, PERFORMANCE, COMPATIBILITY, MERCHANTABILITY, AND/OR FITNESS FOR A PARTICULAR PURPOSE.

6.2 Limitation of Liability. TO THE FULLEST EXTENT PERMITTED BY LAW, THE AGGREGATE LIABILITY OF EACH PARTY (INCLUDING ITS TRUSTEES, DIRECTORS, OFFICERS, EMPLOYEES, AGENTS, CONTRACTORS AND REPRESENTATIVES) IN CONNECTION WITH THE CONSORTIUM LEAD AGREEMENT AND AND THESE TERMS AND CONDITIONS SHALL NOT EXCEED TWO TIMES THE FEES DUE TO ORCID UNDER THE CONSORTIUM LEAD AGREEMENT DURING THE INITIAL TERM OR THEN-CURRENT RENEWAL TERM. IN NO EVENT SHALL THE PARTIES (INCLUDING THEIR TRUSTEES, DIRECTORS, OFFICERS, EMPLOYEES, AGENTS, CONTRACTORS AND REPRESENTATIVES) BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL OR PUNITIVE DAMAGES. FOR THE AVOIDANCE OF DOUBT, ANY PAYMENTS FROM Consortium Lead OR A CONSORTIUM MEMBER TO ORCID IN CONNECTION WITH A CLAIM BY A THIRD PARTY AGAINST ORCID SHALL NOT BE DEEMED TO BE AN INDIRECT OR CONSEQUENTIAL DAMAGE FOR PURPOSES OF THE PRECEDING SENTENCE.

6.3 Consortium Liability. (i) *Consortium Lead* shall ensure that each Consortium Member is fully aware of the terms and conditions of these Terms and Conditions and shall take reasonable steps to ensure that each Consortium Member uses the ORCID Registry and exercises the Member Benefits in compliance with these Terms and Conditions. Consortium Lead shall be liable for its own acts, omissions and breaches under the Consortium Agreement, including, without limitation, its obligations to pay the fees under the Consortium Lead Agreement, its obligations under this Section **6**.3(i), and its representation and warranty that it has the authority to enter into these Terms and Conditions on behalf of each Consortium Member. (ii) Each *Consortium Member* shall be liable for its own acts, omissions and breaches under these Terms and Conditions.

7. Term and Termination.

7.1 Term/Renewal Term. These Terms and Conditions shall continue in effect for the period set forth in the Consortium Lead Agreement. Prior to the end of the the Initial Term or any Renewal Term, ORCID shall provide a renewal notice to Consortium Lead setting forth the expiration date for the then-current term, the dates of the Renewal Term, the relevant fees for the Renewal Term, the due date for such fees, and the list of Consortium Members for the Renewal Term. **Consortium Lead shall have 30 days from the date of such renewal notice to (i) provide a counter-notice to ORCID if it intends not to renew Consortium Agreement or (ii) provide ORCID with an updated list of Consortium members for renewal.** Each Renewal Term shall be term set forth in the renewal notice and shall commence the first day following the end the Initial Term or a Renewal Term (unless otherwise set forth in a renewal notice from ORCID). **A renewal shall not require signature of the parties, and shall be deemed to have occurred if Consortium Lead does not provide a counter-notice of termination within such 30-day period.** Fees and membership will be based on the Consortium Composition set forth in the renewal notice unless Consortium Lead timely provides an updated list of Consortium Members. Failure to make timely payment in absence of a waiver from ORCID shall result in an automatic termination of the Consortium Agreement upon notice from ORCID.

7.2 Termination without Cause. ORCID shall have the right to terminate the Consortium Agreement at the end of the Initial Term or any Renewal Term by providing at least 60 days' notice prior to the end of the then-current term. Consortium Lead may terminate the Consortium Agreement by providing ORCID with a counter notice in response to the renewal notice as described in Section 7.1.

7.3 Termination for Breach. (i) *Termination for cause by Consortium Lead*. In the event that Consortium Lead believes ORCID has materially breached any obligations, representations, or warranties under the Consortium Agreement, it shall so notify ORCID in writing. ORCID shall have 10 days from the receipt of such notice to cure the alleged breach and to notify (in writing) Consortium Lead that such cure has been effected. If the breach is not cured within the 10-day period, Consortium Lead shall have the right to terminate the Consortium Agreement immediately upon written notice. (ii) *Termination for cause by ORCID*. In the event that ORCID believes that Consortium Lead or a Consortium Member has materially breached any obligations, representations, or warranties under these Terms and Conditions (or the Consortium Lead Agreement in the case of Consortium Lead), it shall so notify Consortium Lead in writing. Consortium Lead/Consortium Member shall have 10 days from the receipt of such notice to cure the alleged breach and to notify (in writing) ORCID that such cure has been effected. If the breach is not cured within the 10-day period, ORCID shall have the right to terminate these Terms and Conditions with respect to the Consortium Member immediately upon written notice; provided, however, that if the breaching party is Consortium Lead, ORCID shall have the right to terminate the Consortium Agreement with respect to both Consortium Lead and each Consortium Member. Nothing in this Section 7.3 shall limit ORCID's rights under Section 4.2.

7.4 Effect of Termination. Upon the termination or expiration of these ORCID Terms and Conditions (and/or the Consortium Lead Agreement with respect to Consortium Lead), whichever occurs first, access to the Member API Credentials and Member Benefits for each Consortium Member shall be immediately terminated. (a) *Termination of Specific Member.* If the expiration/termination applies only to a specific Consortium Member (rather than Consortium Lead generally), such Consortium Member shall be removed from Exhibit 1 of the Consortium Lead Agreement, and only such Consortium Member's access to the Member API Credentials and the Member Benefits shall terminate. To the extent that a Consortium Member has deposited/edited any Record Data, such Record Data will remain in the ORCID Registry unless removed by an Individual or designated Trusted Individual(s) and Trusted Organizations before termination, or by ORCID pursuant to Article 5. Notwithstanding the foregoing, each Consortium Member shall have the ability to correct any information it discovers is incorrect after termination by informing ORCID, and ORCID shall seek to promptly correct the inaccuracy with the Individual and/or through the ORCID Dispute Procedures. In the event of termination or expiration of a specific Consortium Member, these Terms and Conditions shall not automatically terminate with respect to Consortium Lead or the other Consortium Members. (b) *Termination of Consortium Lead.* If the expiration/ termination applies to Consortium Lead, ORCID shall have the option of terminating each Consortium Member's rights hereunder as well, in which case it will allow each non-breaching Consortium Member to enter into a separate membership agreement directly with ORCID at the individual member rate.

7.5 Survival. The provisions of Section 1.3(ii) (correction of Record Data), Section 1.3(iv) (License to ORCID), Section 1.**8** (ii) (use of Limited Access Data), Section 1.9 (Limitations on ORCID's Use), Section 2.1 (Ownership of ORCID Registry and Marks), the last sentence of Section 2.2 (use of ORCID Trademark), Article 5 (Dispute Procedures), Article 6 (General Representations and Warranties, Disclaimers, and Limitation of Liability), this Article 7 (Term and Termination), Article **8** (Miscellaneous) and Article 9 (Definitions) shall survive any termination or expiration of Consortium Agreement, including without limitations, these Terms and Conditions and continue in effect.

8. Miscellaneous.

8.1 Entirety of the Agreement. The Consortium Agreement, including these Terms and Conditions, constitutes the entire agreement between Consortium Lead and ORCID and shall supersede any prior written or oral understandings with respect to its subject matter. These Terms and Conditions constitute the entire agreement between ORCID and each Consortium Member and shall supersede any prior oral or written understandings with respect to its subject matter. If the parties have entered into Standard Contractual Clauses related to the transfer and processing of personal data, such clauses shall be an integral part of the agreement as well.

8.2 Agreement Modifications. In order to account for the evolution of ORCID and its sustainability and to operate in compliance with the laws in multiple jurisdictions, ORCID reserves the right to modify these Terms and Conditions, provided that (i) no such modification will be retroactive; and (ii) ORCID will provide Consortium Lead with 60 days' advance written notice of any such modifications. Continued acceptance of these Terms and Conditions is a condition of the

Member Benefits and the licenses granted hereunder. If Consortium Lead objects to any such modifications, Consortium Lead may terminate the Consortium Agreement (effective as of the effective date of such modifications) by providing written notice to ORCID prior to the effective date, and ORCID will provide Consortium Lead with a pro-rata refund. Except as set forth in this Section **8**.2 or referenced elsewhere in these Terms and Conditions (e.g., increases in the Member Benefits, update of contact information) and the policies incorporated herein (e.g., the Privacy Policy, the ORCID Dispute Procedures), all amendments to the Consortium Agreement or any part thereof must be made in writing and signed by ORCID and Consortium Lead.

8.3 Notices. Any notice required to be given by ORCID under the Consortium Agreement or any part thereof shall be given only to Consortium Lead's Main Contact. It is Consortium Lead's responsibility to keep its contact information up to date and to timely forward any such notice to each Consortium Member. All notices given (by or to ORCID) pursuant to the Consortium Agreement or ORCID's bylaws shall be in writing in English and sent as follows: (i) by internationally recognized courier (e.g., FedEx, UPS), or (ii) by electronic mail. Notice shall be deemed given and received on the next business day following the scheduled delivery date for courier and the next business day following the date sent for electronic mail. Either ORCID or Consortium Lead may from time to time change the name and contact information on the Consortium Lead Agreement and on the Consortium Member List by providing notice to the other party in accordance with this Section.

8.4 Disputes/Governing Law. The Consortium Agreement, or any part thereof, shall be interpreted under and governed by the laws of the State of New York, United States, excluding any laws that might direct the application of the laws of another jurisdiction. The application of the United Nations Convention on Contracts for the International Sale of Goods is expressly excluded, if applicable. Except as set forth in the ORCID Dispute Procedures (which shall govern the disputes described therein), if the parties cannot resolve any disputes arising out of or relating to any aspect of the Consortium Agreement in an amicable manner, they shall do so through a desk arbitration administered by the American Arbitration Association in the case of domestic disputes and the International Centre for Dispute Resolution of the American Arbitration Association in the case of international disputes (either, the "AAA") governed by its applicable rules, as modified by the following: (i) regardless of the amount in controversy, the matter shall be determined by one arbitrator familiar with the information technology sector based upon written submissions in English and one or more telephonic hearings in English (as determined by the arbitrator); (ii) the parties shall submit documents pertaining to the arbitration consistent with AAA rules and as directed by the arbitrator; and (iii) the arbitrator shall render a final binding decision 14 days after the arbitrator declares the hearing closed. A judgment on the award rendered by the arbitrator may be entered in any court having competent jurisdiction thereof. Notwithstanding the foregoing, any party may apply to the arbitrator seeking injunctive relief until the arbitration award is rendered or may, without waiving any remedy under any aspect of the Consortium Agreement, seek from any court located in New York, New York, United States (and ORCID, Consortium Lead and each Consortium Member consents to such jurisdiction) injunctive or any other type of equitable relief that is necessary to protect the rights or property of that party, pending arbitration or final determination of the merits of the controversy via arbitration. Consortium Lead and Consortium Members acknowledge that unauthorized use of the Member API Credentials, the ORCID Registry, and/or security breaches might cause ORCID irreparable harm.

8.5 Limitation on Assignment. Except as expressly set forth herein, no party may assign, subcontract or sublicense (collectively, "transfer") its rights and obligations under any aspect of the Consortium Agreement in whole or in part, without the prior written consent of Consortium Lead (for Consortium Lead or Consortium Member) or ORCID, as relevant, which shall not be unreasonably withheld, and any transfer to the contrary shall be null and void; provided, however, that a transfer by ORCID (including, without limitation, transfer by ORCID of the ORCID Registry) in the event of a merger, other corporate restructuring or dissolution, shall be permissible without prior consent, provided that (a) the transferee agrees to be bound by the terms of and conditions of the Consortium Agreement, (b) notice is provided to Consortium Lead (for Consortium Lead or Consortium Member), and (c) such assignee is a nonprofit entity capable of fulfilling ORCID's obligations hereunder and is consistent with ORCID's obligations under its Privacy Policy.

8.6 No Agency, Joint Venture or Partnership. Nothing contained in any aspect of the Consortium Agreement shall be deemed to create an agency, joint venture, or partnership. (Notwithstanding anything to the contrary herein, these Terms and Conditions are not intended to impact any pre-existing such relationship between Consortium Lead and Consortium Member.)

8.7 No Third Party Beneficiaries. The Consortium Agreement has been entered into for the sole benefit of ORCID, Consortium Lead and the Consortium Members and is not intended for the benefit of any third party, regardless of any laws to the contrary.

8.8 Waiver or Invalidity of any Provision. Waiver of any provision of the Consortium Agreement shall not be

deemed to be a waiver of any other provision thereof, nor shall waiver of any breach of any aspect of the Consortium Agreement be construed as a continuing waiver of other breaches of the same or other provisions of thereof If any provision(s) of the Consortium Agreement is held to be invalid, illegal, unenforceable, or in conflict with the law of any jurisdiction, the validity, legality, and enforceability of the remaining provisions shall not in any way be affected or impaired.

8.9 Force Maieure. No party shall be in breach of any aspect of the Consortium Agreement to the extent a failure to perform an obligation hereunder results from a condition(s) that is beyond such party's reasonable control, including, but not limited to, strikes, labor disputes, terrorist acts, or governmental requirements.

8.10 Ethical Behavior. Each party represents and warrants that it has not and shall not, nor to its knowledge has or will any person acting on its behalf, act in violation of applicable anti-bribery and corruption laws in effect in its jurisdiction(s) of operation or its own internal policies related to such matters. Notwithstanding any other provision of theseTerms and Conditions (or the Consortium Lead Agreement), any breach by a party of this Section **8.**10 may be regarded by the other party as incapable of remedy and permitting the non-breaching party, without prejudice to its other rights and remedies, to terminate these Terms and Conditions (or the Consortium Lead Agreement with respect to Consortium Lead and ORCID) immediately upon notice.

8.11 Drafting. The Consortium Agreement shall not be construed or interpreted against ORCID as the drafter.

9. Definitions

API or ORCID API: See Member APIs below.

Consortium Effective Date means the effective date set forth in the Consortium Lead Agreement.

Consortium Agreement means, (i) the document titled ORCID Consortium Lead Agreement, (ii) its Exhibit 1 (ii) these Terms and Conditions, and (iv) the ORCID Member Benefits, the ORCID Privacy Policy and the ORCID Dispute Procedures which are incorporated by reference in these Terms and Conditions.

Consortium Composition means the number of Consortium Members and the fee tier of each member.

Consortium Lead Agreement means the agreement executed by the Consortium Lead and ORCID effective as of the Consortium Effective Date.

Consortium Member List means the list in the ORCID online service tool of current Consortium Members as updated by Consortium Lead from time to time and accepted by ORCID.

Effective Date means for each Consortium Member, the date on which Consortium Lead adds Consortium Member to the Consortium Member List (with the acceptance of ORCID). For Consortium Lead, the Effective Date means the Consortium Effective Date (as defined in the Consortium Lead Agreement).

Individual means a person about whom an ORCID Record exists or is being created.

Initial Term means the duration of these Terms and Conditions as set forth in the Consortium Lead Agreement.

Limited Access Data means Record Data that is viewable through the ORCID Registry only by the Individual, a Trusted Individual or specified Trusted Organizations.

Member means any organization that has entered into these Terms and Conditions with ORCID relating to use of the ORCID Registry, Member API Credential(s), and the Member APIs, or otherwise meets conditions established by ORCID.

Member APIs means APIs which interact with the ORCID Registry through Member API Credential(s).

Member API Credential(s) means a unique passcode provided by ORCID to each Consortium Member to use the Member APIs.

Member Benefits means the use of the aspects of the ORCID Registry only available to ORCID members as described in Article 1 of these Terms and Conditions and on the ORCID website as amended by ORCID from time to time.

ORCID Identifier means the globally unique identifier assigned by ORCID to an Individual.

ORCID Dispute Procedures means the procedures ORCID uses to assist Members and other users of the ORCID Registry to resolve disputes about the accuracy of Record Data, posted on the ORCID website at https://info.orcid.org/dispute-procedures/, as amended from time to time by ORCID.

ORCID Record means the information about an Individual in the ORCID Registry other than System Data.

ORCID Registry means the ORCID database that contains all Record Data.

Privacy Policy means those privacy practices and commitments made by ORCID and that are posted by ORCID under the title "Privacy Policy" on the ORCID website at https://info.orcid.org/privacy-policy/, as amended from time to time by ORCID.

Privacy Settings means selections indicating whether specific data within a Record shall be *Private Data*, *Limited Access Data*, *or Public Data*. (For additional information about Privacy Settings, please see the Privacy Policy.)

Public API Credential means a unique passcode to access the free ORCID Public API, which allows individuals that are not affiliated with ORCID Members to connect their systems and applications to the ORCID Registry with machine-to-machine communication and read public data.

Public Data File means a downloadable file of all Public Data in the ORCID Registry on a given date from Records created or claimed by an Individual.

Record Data means the individual data elements in a Record, including the ORCID Identifier and metadata associated with linked research objects. A link, but not the linked object itself (e.g., text or full metadata), is considered part of the Record Data.
Renewal Term means each successive term following the Initial Term.
System Data means data associated with a Record that is not part of the visible ORCID Registry, such as a password.
Terms and Conditions means these ORCID Membership Terms and Conditions.
Trusted Individual means a person to whom an Individual has given the authority to manage an ORCID record on his or her behalf, including setting privacy settings, editing and depositing data and naming Trusted Organizations.
Trusted Organization means a Member that has been granted rights by an Individual (or his/her Trusted Individual(s)) to deposit
and edit Record Data and/or read Record Data that has been marked "Limited Access".
Use means use, store, sublicense, reproduce, modify, transmit, distribute, publicly perform and publicly display, including for commercial use.

Smlouva o vedení konsorcia

Koordinátor konsorcia: Národní technická knihovna
Typ entity: Státní příspěvková organizace zřízená Ministerstvem školství, mládeže a tělovýchovy v České republice
Místo: Technická 2710/6, 160 80 Praha 6 – Dejvice
IČO: 61387142

Tato smlouva o vedení konsorcia je uzavřena mezi společností ORCID, Inc., neakciovou společností z Delawaru, se sídlem 10411 Motor City Drive, Suite 750, Bethesda, MD 20817 USA („ORCID"), a Vedoucím konsorcia ke dni účinnosti konsorcia (jak je definován níže). S ohledem na vzájemné závazky obsažené v této smlouvé a za přiměřené protiplnění, se Vedoucí konsorcia a ORCID tímto dohodli na podmínkách a povinnostech uvedených níže, v Příloze 1 a v Podmínkách členství v konsorciu ORCID (dále jen „Smluvní podmínky"), které jsou přiloženy k této smlouvé a jsou do ní začlenény odkazem. **Pojmy s velkými písmeny, které nejsou definovány jinde, jsou definovány v článku 9 Smluvních podmínek.**

	Vedoucí konsorcia Hlavní kontaktní osoba	**Vedoucí konsorcia Kontaktní osoba pro administrativu**	**Vedoucí konsorcia Kontaktní osoba pro technické záležitosti**
Jméno			
Funkce			
Adresa			
E-mail			
Telefon			

Hlavní kontaktní osoba ORCID:

Ivo Wijnbergen, Director of Engagement, ORCID, Inc., 10411 Motor City Drive, Suite 750, Bethesda, MD 20817, USA; membership@orcid.org; [redacted]

Počáteční období: 01/06/2023 **(„datum účinnosti konsorcia") do 31/05/2024, s výhradou ukončení a obnovení, jak je uvedeno ve Smluvních podmínkách.**

Členové konsorcia: Jak je dále popsáno v Příloze 1 (přiložené k tomuto dokumentu a začlenéné do něj odkazem), Vedoucí konsorcia udržuje seznam (dále jen „Seznam členů konsorcia") subjektů (dále jen „Člen konsorcia" a společné „Členové konsorcia") prostřednictvím samoobslužného nástroje ORCID na adrese http://orcid.org/self-service, včetné Vedoucího konsorcia, pokud je to relevantní, které mají být Členy ORCID a mají nárok na Členské výhody. Vedoucí konsorcia vyplní Seznam prvních členů konsorcia před Datem účinnosti. Následné může Vedoucí konsorcia Seznam členů konsorcia průběžné aktualizovat. Každý navrhovaný subjekt se stane Členem konsorcia po přijetí ze strany ORCID.

Vedoucí konsorcia prohlašuje a zaručuje, že má veškerou nezbytnou pravomoc a oprávnění k tomu, aby (i) svým vlastním jménem uzavřel tuto Smlouvu o vedení konsorcia a Smluvní podmínky, (ii) jednal jako zástupce a zavazoval každého člena konsorcia stanoveného v seznamu členů ve Smluvních podmínkách a že podpisem této Smlouvy o vedení konsorcia budou tyto Smluvní podmínky právné závazné pro vedoucího konsorcia a každého člena konsorcia uvedeného na seznamu členů konsorcia.

Pouze vysokoškolské instituce, neziskové organizace a vládní výzkumné a výzkum financující agentury se sídlem v České republice a zřízené podle zákonů České republiky jsou oprávněny čerpat Členské výhody za zde stanovenou výši konsorciálního poplatku (definovaného níže) a Vedoucí konsorcia prohlašuje a zaručuje, že každá instituce uvedená na Seznamu členů konsorcia je takovým subjektem.

Platební podmínky:

Klasifikace ORCID: **Konsorcium**

Počáteční Složení konsorcia: *(počet členů na úroveň; doplní ORCID)*
Počáteční Poplatek konsorcia: *(vyplní ORCID)*

Vedoucí konsorcia bude odpovědný za vybírání a zaplacení ročního členského poplatku (dále jen „Poplatek konsorcia“) ORCID uvedenému v sazebníku poplatků na webových stránkách ORCID https://info.orcid.org/membership podle počtu členů konsorcia a výše poplatků každého člena („Složení konsorcia“).

Konsorciální poplatek je splatný 45 dní od podpisu této Smlouvy o vedení konsorcia. Pokud Vedoucí konsorcia přidá během Počátečního období nebo Období obnovení jakékoli další Členy konsorcia, což povede ke zvýšení Složení konsorcia, jak je uvedeno výše, bude ORCID účtovat dodatečné poplatky na poměrném základě, které budou splatné 45 dní po přidání takového člena konsorcia.

Poplatky za obnovení jsou splatné přesné 45 dní od data uvedeného v roční faktuře zaslané ORCID. Snížení nebo zvýšení poplatků na základě složení konsorcia bude vyhodnoceno při každém Období obnovení.

Všechny platby budou provedeny v amerických dolarech. Jakékoli nezpochybněné platby provedené více než šedesát (60) dnů po jejich splatnosti, budou podléhat 1,5% měsíčnímu úrokovému poplatku a ORCID si vyhrazuje právo zmrazit přístup k Členských oprávnění API Členů konsorcia, dokud nebudou provedeny nezpochybněné platby. Všechny platby budou provedeny vzájemně přijatelnou formou bankovního převodu na ORCID, kreditní kartou nebo šekem splatným společnosti ORCID Inc.

Z Poplatků konsorcia splatných společnosti ORCID se neodečítají žádné daňové srážky. Pokud Poplatek konsorcia podléhá jakémukoli zdanění (jinému než zdanění příjmu ORCID ve Spojených státech), pak je Vedoucí konsorcia odpovědný za (i) náklady na takovou daň a (ii) mimo Spojené státy za odvedení této dané všude tam, kde je to právně přípustné.

Společnost ORCID si vyhrazuje právo účtovat dodatečné poplatky za jakékoli další Členské výhody, které budou k dispozici a které se Vedoucí konsorcia rozhodne licencovat jménem Členů konsorcia během Počátečního období nebo Obnoveného období. Pokud bude v Seznamu členů konsorcia kdykoli během Počátečního období nebo Obnoveného období méně než 5 Členů konsorcia, budou Poplatky konsorcia upraveny na standardní poplatky za přímé členství v ORCID a sleva se s okamžitou platností přestane uplatňovat. Roční navýšení Poplatků konsorcia bude obecně činit maximálně 3 % ročně (bez ohledu na změny ve Složení Konsorcia nebo zaokrouhlování poplatků na Člena) a společnost ORCID oznámí Vedoucímu členovi Konsorcia každé takové navýšení poplatků nejméně 60 dní předem. Společnost ORCID si vyhrazuje právo průběžně restrukturalizovat model Poplatků konsorcia podle svého uvážení, a pokud takové změny povedou k navýšení Poplatku konsorcia o více než 3 %, které není způsobeno změnami ve Složení konsorcia, oznámí společnost ORCID každou takovou změnu nejméně 12 měsíců předem. Bez ohledu na oddíl 6.2 Smluvních podmínek bude Vedoucí Konsorcia odpovědný za veškeré prokazatelné, přímé a přiměřené náklady a výdaje (mimo jiné včetně přiměřených poplatků za právní zastoupení), které společnosti ORCID vzniknou při vymáhání jakýchkoli dlužných částek.

Používání ochranné známky: ORCID je komunitní iniciativa, a proto chce propagovat účast svých Členů. Za tímto účelem, pokud je níže zaškrtnuto políčko „souhlasím“, může společnost ORCID během Počátečního období a jakéhokoli Prodlouženého období používat název a loga Vedoucího konsorcia v rozsahu toho, že Vedoucí konsorcia a společnost ORCID uzavřely tuto Smlouvu o vedení konsorcia, pro identifikaci Vedoucího konsorcia jako člena ORCID (je-li to relevantní) a pro sdílení jakýchkoli odkazů, které Vedoucí konsorcia vytvoří, z webových stránek Vedoucího konsorcia na webové stránky ORCID.

☐ Souhlasím

Vedoucí konsorcia je oprávněn a vyzván k používání názvu, loga a dalších ochranných známek ORCID (dále jen „označení“) za účelem oznámení konsorcia ORICD a svého statusu Vedoucího konsorcia za předpokladu, že na žádost ORCID tato označení správně označí jako ochrannou známku podle zákonů USA a dalších zákonů. (Viz Pokyny pro zobrazování ochranných známek a ID na webových stránkách ORCID.) Vedoucí konsorcia nesmí používat označení způsobem, který by mohl vyvolat záměnu původu zboží nebo služeb nebo naznačovat podporu ze strany ORCID, s výjimkou případů, kdy to ORCID výslovně písemně schválí.

Podpora:

Poplatek konsorcia pokrývá poskytování Členských oprávnění API pro každého Člena konsorcia uvedeného na Seznamu členů konsorcia a podporu ORCID uvedenou v dokumentu *Role a povinnosti konsorcií ORCID* (dostupné na https://info.orcid.org/orcid-for-consortia/roles-and-responsiblities/). Vedoucí konsorcia bere na vědomí (i) role a povinnosti Vedoucího konsorcia stanovené v dokumentu *Role a povinnosti konsorcií ORCID* a souhlasí s tím, že do 90 dnů od Data účinnosti konsorcia zavede příslušnou podporu a služby (mimo jiné včetné technické podpory poskytované vedoucím konsorcia); a (ii) Poplatek konsorcia je založen na tom, že Vedoucí konsorcia bude tyto služby poskytovat, a neposkytnutí téchto služeb by mohlo vést ke zvýšení Poplatku konsorcia.

Oznámení:

Veškerá oznámení, která má ORCID podle Smluvních podmínek učinit, se podávají pouze hlavní kontaktní osobě Vedoucího konsorcia. Vedoucí konsorcia odpovídá za aktuálnost svých kontaktních údajů a za včasné předání všech takových oznámení Členům konsorcia.

Různé: Oddíly 8.3 až 8.10 Smluvních podmínek se vztahují i na konstrukci, výklad a vymáhání této Smlouvy o vedení konsorcia jako součást Smlouvy o poskytnutí služeb ORCID. V případě přímého rozporu se tato Smlouva o vedení konsorcia bude řídit Smluvními podmínkami.

Tato Smlouva o vedení konsorcia a případné dodatky jsou vyhotoveny v jednom nebo více stejnopisech, z nichž každý bude považován za originál, ale všechny budou tvořit jednu smlouvu. **KAŽDÁ ZE STRAN MŮŽE POUŽÍT FYZICKÝ NEBO ELEKTRONICKÝ PODPIS, PŘIČEMŽ KAŽDÝ Z NICH SE POVAŽUJE ZA VĚROHODNÝ A STEJNĚ VYMAHATELNÝ.**

Tato dohoda je vyhotovena ve dvou stejnopisech v českém a anglickém jazyce pro každou ze smluvních stran, přičemž obé vyhotovení mají platnost originálu. V případě jakýchkoli rozporů nebo nesrovnalostí mezi českou a anglickou verzí této smlouvy má přednost anglická verze.

NA DŮKAZ VÝŠE UVEDÉHO ORCID a Vedoucí konsorcia prohlašují, že tato Smlouva o vedení konsorcia byla uzavřena řádně oprávněným zástupcem, ve spojitosti s uzavřením Smlouvy o poskytnutí služeb ORCID.

[JMÉNO VEDOUCÍHO KONSORCIA]	ORCID, Inc.
Podpis: _____	Podpis: _____
Jméno: _____	Jméno: Chris Shillum
Funkce: _____	Funkce: Jednatel
E-mailová adresa: _____	E-mailová adresa: [redacted]
Datum: _____	Datum: _____

Příloha č. 1 Smlouvy o vedení konsorcia: Členové konsorcia

Vedoucí konsorcia vede Seznam členů konsorcia prostřednictvím samoobslužného nástroje ORCID na adrese http://orcid.org/self-service včetně níže uvedených informací. Vedoucí konsorcia by měl uvěst i svůj název, pokud se stává členem ORCID. Vedoucí konsorcia je odpovědný za to, že Seznam členů konsorcia je stále aktuální a přesný.

- **Název organizace**
- **Hlavní kontaktní osoba: Jméno, pracovní pozice, e-mail.** Hlavní kontaktní osoba uvedená u každého člena konsorcia je osoba, která zastupuje Člena konsorcia pro účely (i) oznámení podle Smluvních podmínek a stanov ORCID a (ii) hlasování o členství a která jinak jedná jménem Člena konsorcia podle Smluvních podmínek a stanov ORCID.
- **Kontaktní osoba pro technické záležitosti: Jméno, pracovní pozice, e-mail.** Kontaktní osoba pro technické záležitosti je osoba odpovědná za správu Členského oprávnění API.

Vedoucí konsorcia navíc vede sdílený samostatný dokument na následující adrese www.identifikatorv.cz s následujícími informacemi:

- **Název organizace**
- **Adresa organizace**
- **Licence na ochrannou známku:** Uveďte „ano“, pokud může ORCID během Počátečního období a jakéhokoli Prodlouženého období používat název a loga příslušného Člena konsorcia pro omezené účely označení, že Člen konsorcia je členem ORCID, a pro propagaci jakýchkoli odkazů, které člen konsorcia vytvoří ze svých webových stránek na webové stránky ORCID. Pokud taková licence není udělena, uveďte „ne“.

Podmínky členství v konsorciu ORCID

ORCID, Vedoucí konsorcia (dále jen „Vedoucí konsorcia“) a každý subjekt (dále jen „Člen konsorcia“) uvedený na Seznamu členů konsorcia, jak je popsáno v Příloze **1** ke Smlouvě o vedení konsorcia, jež je podepsaná Vedoucím konsorcia a účinná od Data účinnosti konsorcia, jsou vázáni těmito podmínkami členství v konsorciu ORCID (dále jen „Smluvní podmínky“), které odkazem zahrnují Zásady ochrany osobních údajů ORCID, Postupy pro řešení sporů ORCID a Členské výhody.

1. Udělení licence od ORCID a Členské výhody. Každý Člen konsorcia má Členské výhody, které jsou k dispozici prémiovým členům ORCID a které zahrnují minimálně výhody uvedené v tomto článku **1**. Společnost ORCID může průběžně přidávat a měnit Členské výhody nad rámec výhod uvedených v tomto článku **1** a aktuální Členské výhody jsou uvedeny na internetových stránkách společnosti ORCID. Všechny Členské výhody podléhají těmto Smluvním podmínkám. Licence uvedená v oddíle **1.1** a ostatní Členské výhody zůstávají v platnosti po Počáteční období (nebo příslušně Prodlouženě období) stanoveně ve Smlouvě o vedení konsorcia (nebo v oznámení o prodloužení), pokud nejsou dříve ukončeny podle oddílu 7 nebo omezeny podle oddílu 4.2.

1.1 Udělení licence: Od Data účinnosti a za předpokladu, že Vedoucí konsorcia včas a v plně výši uhradí Poplatky stanoveně ve Smlouvě o vedení konsorcia, uděluje ORCID každému Členovi konsorcia nepřevoditelnou licenci k používání Členských oprávnění API k přístupu k členským rozhraním API a ke čtení, ukládání/úpravě a používání Záznamových dat v souladu s příslušnými nastaveními ochrany osobních údajů a těmito Smluvními podmínkami. Všechna práva, která zde nejsou výslovně uvedena, si vyhrazuje společnost ORCID. Žádný z těchto dokumentů nevyžaduje, aby Člen konsorcia využíval některou z Členských výhod.

1.2 Členové konsorcia, kteří jsou poskytovateli služeb.
V tomto dokumentu se „poskytovatelem služeb“ rozumí organizace, která poskytuje služby nebo produkty jiným organizacím na základě používání svých Členských oprávnění API, jiných Členských výhod nebo vytváření či ověřování Identifikátorů ORCID. Poskytovatelé služeb musí od svých zákazníků vyžadovat, aby používali vlastní oprávnění API, ať už ve formě bezplatného Veřejného oprávnění API, nebo placeného Členského oprávnění API. ORCID si vyhrazuje právo rozhodnout, zda aplikace vyžaduje samostatný certifikát API, a proto se poskytovatelům služeb doporučuje, aby své plány s ORCID projednali předem.

1.3 Úschova/úprava dat. Každý Člen konsorcia má možnost ukládat a upravovat Záznamová data ve stávajících Záznamech ORCID, pokud příslušná osoba udělila Členovi konsorcia oprávnění jako Důvěryhodné organizaci, a to za následujících podmínek:
(i) Každý Člen konsorcia ukládá/upravuje pouze ten typ a rozsah Záznamových dat, pro který má souhlas fyzické osoby prostřednictvím mechanismu ORCID pro udělování souhlasu Důvěryhodným organizacím.
(ii) Každý Člen konsorcia ukládá/upravuje pouze taková Záznamová data, které jsou podle jeho nejlepšího vědomí v době ukládání/úpravy pravdivé a správné a jsou spojeny se správnou osobou a Identifikátorem ORCID. Pokud se Člen konsorcia po uložení/úpravě dozví, že údaje v Záznamu ORCID, které uložil/upravil, jsou nesprávné, opraví je nebo informuje příslušnou osobu a ORCID. Člen konsorcia není povinen aktualizovat Záznamová data jinak než opravou Záznamových dat, které nebyly v době uložení/úpravy pravdivé a správné, nebo informováním ORCID a příslušné osoby o tom, že tato Záznamová data jsou nesprávná, a nenese žádnou odpovědnost za to, že ORCID nadále používá neopravená Záznamová data poté, co je Člen konsorcia opravil nebo informoval příslušnou osobu a ORCID.
(iii) Pokud Člen konsorcia ukládá/upravuje odkazy na články, blogy, soubory dat nebo jiná díla, která mohou podléhat ochraně duševního vlastnictví, musí tak činit pouze způsobem, který podle jeho vědomí neporušuje autorská práva nebo jiná práva duševního vlastnictví třetí strany.
(iv) V souladu s těmito Smluvními podmínkami uděluje každý Člen konsorcia společnosti ORCID bezplatnou, nevýhradní, celosvětovou, trvalou a neodvolatelnou licenci na veškerá práva potřebná k tomu, aby společnost ORCID a veřejnost mohla používat tato uložená/upravená Záznamová data, s výhradou případných Nastavení ochrany osobních údajů.

1.4 Vyhledávání dat, stahování dat a s tím související upozornění. Každý Člen konsorcia má přístup k členským rozhraním API, aby mohl nahlížet do registru ORCID a stahovat Záznamová data, včetně údajů s omezeným přístupem, pokud mu příslušné fyzické osoby nebo Důvěryhodné osoby udělí právo. Kromě toho má každý Člen konsorcia přístup k mechanismu pro pravidelnou synchronizaci změn ve Veřejném datovém souboru.

1.5 Technická podpora. ORCID poskytne Vedoucímu konsorcia a Členům konsorcia technickou podporu stanovenou v dokumentu *Role a povinnosti konsorcia ORCID* (k dispozici na https://info.orcid.org/orcid-for-consortia/roles-and-responsiblities/). Technická podpora musí být koordinována prostřednictvím kontaktní osoby pro technické záležitosti ve Smlouvě o vedení konsorcia a v prohlášení o *rolích a povinnostech*.

1.6 Prosazování ochrany soukromí. Pokud Člen konsorcia vyžaduje používání Identifikátorů ORCID a umožňuje jejich shromažďování pomocí rozhraní API ORCID, má Člen konsorcia právo, nikoli však povinnost, prosazovat jménem jakékoli fyzické osoby, kterou pověřil používáním Identifikátoru ORCID, závazky ORCID týkající

se ochrany osobních údajů vůči této fyzické osobě, jak je uvedeno v zásadách ochrany osobních údajů ORCID.

1.7 Nominace do správní radv ORCID a účast na řízení. Osoby zastupující každého Člena konsorcia mohou vykonávat hlasovací práva Člena konsorcia a být nominovány do správní rady ORCID v souladu se stanovami ORCID, které jsou k dispozici na internetových stránkách ORCID. Osoba uvedená Vedoucím konsorcia jako hlavní kontaktní osoba na Seznamu členů konsorcia pro každého Člena je osobou, jež zastupuje Člena konsorcia pro účely oznámení, hlasování o členství a jiného výkonu práv Člena konsorcia podle stanov ORCID. (Člen konsorcia může změnit jméno hlavního kontaktu prostřednictvím oddělení podpory Vedoucího konsorcia.)

1.8 Omezení užití pro Členv konsorcia. Každý Člen konsorcia souhlasí s následujícími omezeními:

(i) Neumožnit žádnému jinému subjektu používat jeho Členské oprávnění API s výjimkou případů, kdy tak Člen konsorcia pověřil daný subjekt v souladu s témito Smluvními podmínkami;

(ii) Nezveřejňovat žádné jiné osobě nebo subjektu Data s omezeným přístupem, pokud (a) tato Data nejsou veřejné dostupná z jiného zdroje nebo (b) Člen konsorcia neoznámí fyzické osobě, jak a komu budou tato Data zpřístupněna;

(Iii) Neukládat/neupravovat jiné typy dat, než které jsou povoleny v daném poli, a nezahrnovat do těchto polí plná díla (jinými slovy, lze ukládat pouze metadata a odkazy na díla, nikoli texty článků, blogy nebo publikace a datové sady);

(iv) Neukládat ani neupravovat žádný Záznam ORCID způsobem, který by jej vědomé učinil nepravdivým, zavádějícím nebo pomlouvačným, a to vcelku nebo zčásti, ani vědomé nepoužívat žádný Záznam ORCID způsobem, který by porušoval výše uvedené nebo práva na publicitu nebo soukromí jakékoli osoby;

(v) Nepoužívat žádná Záznamová data ke kontaktování osob pro marketingové účely, aniž by tato osoba měla právo se z takové marketingové komunikace odhlásit;

(vi) Nepoužívat Záznamová data k rozesílání nevyžádané pošty, spamu, řetězových dopisů, pyramidových schémat nebo podobných schémat;

(vii) Nepoužívat Záznamová data k obtěžování, zneužívání nebo poškozování jiné osoby;

(viii) Nepřekonávat, neobcházet ani nezakázat žádné šifrovací funkce nebo softwarové ochrany používané k ochrané bezpečnosti Členského oprávnění API, Registru ORCID nebo Záznamových dat;

(ix) Nemanipulovat s Identifikátory ORCID za účelem zakrytí původu jakýchkoli Záznamových dat; vědomé nenahrávat nebo nezveřejňovat žádná Záznamová data, která obsahují softwarové viry nebo jakýkoli jiný počítačový kód, soubory nebo programy určené k přerušení, zničení nebo omezení funkčnosti jakéhokoli softwaru, hardwaru nebo telekomunikačního zařízení; nebo úmyslné zasahovat do serverů nebo sítí ORCID nebo je narušovat;

(x) Nepoužívat žádné Členské oprávnění API nebo jeho Členské výhody k vytvoření služby nebo produktu, který umožňuje organizacím získat užitky těchto Členských výhod, aniž by se jednalo o členy ORCID; a

(xi) Nepoužívat žádné Členské oprávnění API, Členské výhody, členské rozhraní API nebo Registr ORCID v rozporu s témito Smluvními podmínkami nebo způsobem, který je jinak nezákonný ve Spojených státech amerických („USA“) a v jurisdikci, v níž se Člen konsorcia nachází, pokud se jedná o jinou jurisdikci než USA.

1.9 Omezení Používání ORCID. ORCID bude používat a zpřístupňovat Záznamová data prostřednictvím Registru ORCID a Veřejný datový soubor pouze v souladu s témito Smluvními podmínkami a v rozsahu, v jakém budou Záznamová data upravena nebo odstraněna v souladu s témito Smluvními podmínkami, budou tyto změny zohledněny v zobrazitelném Registru ORCID a budoucích Veřejných datových souborů.

2. Duševní vlastnictví.

2.1 Vlastnictví Registru ORCID a označení ORCID. Mezi stranami vlastní ORCID veškerá práva, tituly a podíly, mimo jiné včetně příslušných databázových práv, Registru ORCID a softwaru vyvinutého společností ORCID, Systémová data, členské API, Členské oprávnění API a označení ORCID, jak jsou definovány v oddíle 2.2 (souhrnné „Duševní vlastnictví ORCID“); za předpokladu, že duševní vlastnictví ORCID nezahrnuje žádné jednotlivé datové prvky v Registru ORCID. ORCID poskytuje svůj software registru pod licencí open source, kdykoli je to legálně možné. (Viz Open Source Project na webových stránkách ORCID.)

2.2 Používání ochranných známek ORCID. Člen konsorcia je oprávněn k používání názvu, loga a dalších ochranných známek ORCID (dále jen „označení“) k oznámení používání Registru ORCID a statusu člena ORCID za předpokladu, že Člen konsorcia na žádost ORCID správně označí označení jako ochranné známky podle zákonů USA a dalších zákonů. (Viz ORCID Brand Guidelines.) Člen konsorcia nesmí používat označení způsobem, který by mohl vyvolat záměnu ohledně původu zboží nebo služeb nebo naznačovat podporu ze strany ORCID, s výjimkou případů, kdy to ORCID výslovně písemně schválí.

3. Dodání a obecná podpora.

3.1 Nedostupnost Registru ORCID. ORCID vynaloží komerčně přiměřené úsilí, aby zajistila nepřetržitou dostupnost Registru ORCID a Členských výhod. Vedoucí konsorcia a všichni Členové konsorcia berou na vědomí, že Registr ORCID a Členské výhody nemusí být trvale k dispozici z důvodu údržby serveru (serverů), instalace nebo testování softwaru a odstávek souvisejících se zařízením nebo službami mimo kontrolu ORCID, mimo jiné včetně telekomunikačních služeb nebo internetových uzlů či zařízení; ORCID však musí vedoucího konsorcia v

přiměřeném předstihu informovat o všech odstávkách, které jsou pod přiměřenou kontrolou ORCID.

3.2 Prémioví členové. Kromé dalších závazků stanovených v těchto Smluvních podmínkách poskytne ORCID Členovi konsorcia API pro zpětné volání, vyšší počet povolených požadavků na API za den a vlastní zprávy a datové soubory. K prémiovým výhodám patří také možnost, aby každému Členovi konsorcia bylo vydáno až pét (5) Členských oprávnění API pro použití v různých systémových integracích ve stejné organizaci.

4. Ochrana soukromí, zabezpečení a užívání dat.

4.1 Ochrana údajů. Společnost ORCID vynaloží komerčně přiměřené úsilí na ochranu bezpečnosti a integrity Registru ORCID (mimo jiné včetně Členského oprávnění API, hesel, uživatelských jmen a IP adres) a Záznamových dat, jak je uvedeno v jejích Zásadách ochrany osobních údajů, včetně ukládání informací v datovém centru s omezeným přístupem a monitorováním, používání zabezpečených zásuvek a softwaru pro detekci narušení a hashování hesel. ORCID neprodleně informuje Vedoucího konsorcia, jakmile se dozví o jakémkoli závažném narušení bezpečnosti souvisejícím s oprávněními API Člena konsorcia nebo jakmile ORCID zjistí, že došlo k závažnému narušení bezpečnosti Registru ORCID obecně.

4.2 Ochrana Členského oprávnění API, Registru ORCID a Záznamových dat ORCID. Každý Člen konsorcia souhlasí s tím, že bude používat své oprávnění API pouze tak, jak je uvedeno v těchto Smluvních podmínkách, a vynaloží přiměřené úsilí na ochranu svého Členského oprávnění API před jakýmkoli narušením bezpečnosti nebo jiným použitím, které je v rozporu s těmito Smluvními podmínkami nebo platnými právními předpisy. Vedoucí konsorcia nese odpovědnost za své úmyslné pochybení nebo nedbalost při používání Členského oprávnění API, s výjimkou případů, kdy zjistí, že k narušení bezpečnosti došlo vinou společnosti ORCID. Každý Člen konsorcia je odpovědný za své úmyslné pochybení nebo nedbalost při používání svých Členských oprávnění API, s výjimkou případů, kdy prokáže, že k narušení bezpečnosti jeho Členských oprávnění API došlo vinou ORCID. Vedoucí konsorcia a každý Člen konsorcia jsou povinni neprodleně informovat ORCID, jakmile (i) se dozvědí o jakémkoli narušení nebo údajném narušení těchto Smluvních podmínek nebo bezpečnosti Členského oprávnění API nebo Registru ORCID nebo (ii) se dozvědí, že Záznamová data, která Člen konsorcia uložil/upravil, porušují nebo mohou porušovat práva na soukromí, publicitu nebo jiná práva fyzické osoby. Vedoucí konsorcia a každý Člen konsorcia dále plně spolupracují s ORCID při vyšetřování a nápravě narušení nebo údajných narušení, mimo jiné včetně pomoci ORCID při poskytování požadovaných oznámení jednotlivcům. Kromě toho může ORCID (aniž by tím byly omezeny jiné opravné prostředky, jež může ORCID použít) dočasně omezit používání Členského oprávnění API a přístup do Registru ORCID, dokud nedojde k nápravě narušení.

4.3 Monitorování a shromažďování údajiů o Používání. Za účelem ochrany bezpečnosti Členského oprávnění API a Registru ORCID před neoprávněným použitím a za účelem získání informací o Používání Registru ORCID a Členského rozhraní API může ORCID monitorovat činnost a používání Členského oprávnění API a členského rozhraní API.

5. Sporné údaje; stažení údajů z registru ORCID. ORCID pomáhá při řešení sporů mezi uživateli (mimo jiné mezi jednotlivci, Členy konsorcia a dalšími členy) Registru ORCID týkajících se nároků na vlastnictví Identifikátorů ORCID, přesnosti a integrity údajů a identity jednotlivců v souladu se zásadami a postupy stanovenými v postupech řešení sporů ORCID - ORCID Dispute Procedures, které jsou do tohoto dokumentu začleněny odkazem. Bez ohledu na výše uvedené ORCID neposkytuje žádná prohlášení ani záruky o správnosti údajů uložených v Registru ORCID a neodpovídá za ně. ORCID si vyhrazuje právo odstranit z Registru ORCID a jeho serverů jakákoliv Záznamová data nebo zakázat přístup k částem Registru ORCID, pokud to považuje za nezbytné.

6. Obecná prohlášení a záruky, vyloučení odpovědnosti, omezení odpovědnosti. Zástupci Vedoucího konsorcia a ORCID prohlašují a zaručují, že jsou oprávněni uzavřít Smlouvu o vedení konsorcia a tyto Smluvní podmínky a zavázat svou organizaci Smlouvou o vedení konsorcia a těmito Smluvními podmínkami. Vedoucí konsorcia a ORCID prohlašují a zaručují, že zajistily, aby Smlouvu o vedení konsorcia podepsal řádně oprávněný zástupce. Vedoucí konsorcia dále prohlašuje a zaručuje, že je oprávněn jednat jménem každého Člena konsorcia uvedeného v Seznamu členů konsorcia a právně jej zastupovat a zavazovat ke Smlouvě o vedení konsorcia a těmto Smluvním podmínkám a že tak podpisem této smlouvy učinil. S výjimkou případů uvedených v tomto dokumentu ORCID neposkytuje prohlášení ani záruky týkající se (a) přesnosti Záznamových dat; (b) zneužití Záznamových dat; (c) ochrany před pomluvami nebo narušením práv na soukromí v důsledku používání Záznamových dat; (d) absence virů, chyb nebo jiných poškození počítačových systémů a softwaru; a (e) odkazů na jiné webové stránky a obsah na nich.

6.1 Odmítnutí odpovědnosti. KROMĚ VÝSLOVNÝCH PROHLÁŠENÍ A ZÁRUK UVEDENÝCH V TÉCHTO SMLUVNÍCH PODMÍNKÁCH, REGISTR ORCID, ZÁZNAMOVÁ DATA, VEŘEJNÝ DATOVÝ SOUBOR, ČLENSKÉ OPRÁVNĚNÍ API, ČLENSKÉ API A/NEBO ČLENSKÉ VÝHODY (jednotlivě i společně „SYSTÉM ORCID“) JSOU POSKYTOVÁNY NA ZÁKLADĚ „JAK STOJÍ A LEŽÍ“. ORCID A JEJÍ ŘEDITELÉ, ZAMĚSTNANCI, AGENTI, DODAVATELÉ A ZÁSTUPCI (jednotlivě i společně „STRANY ORCID“) SE V NEJVYŠŠÍM ROZSAHU POVOLENÉM ZÁKONEM ZŘÍKAJÍ

JAKÝCHKOLI A VEŠKERÝCH DALŠÍCH ZÁVAZKŮ A ZÁRUK (VÝSLOVNÝCH, PŘEDPOKLÁDANÝCH, ÚSTNÍCH NEBO PÍSEMNÝCH) TÝKAJÍCÍCH SE SYSTÉMU ORCID, MIMO JINĚ VČETNĚ JAKÝCHKOLI A VŠECH PŘEDPOKLÁDANÝCH ZÁRUK KVALITY, VÝKONU, KOMPATIBILITY, PRODEJNOSTI A/NEBO VHODNOSTI PRO KONKRÉTNÍ ÚČEL.

6.2 Omezení zodpovědnosti. V MAXIMÁLNÍM ROZSAHU POVOLENÉM ZÁKONEM NESMÍ CELKOVÁ ODPOVĚDNOST KAŽDÉ STRANY (VČETNĚ JEJÍCH SPRÁVCŮ, ŘEDITELŮ, ÚŘEDNÍKŮ, ZAMĚSTNANCŮ, AGENTŮ, DODAVATELŮ A ZÁSTUPCŮ) V SOUVISLOSTI S SMLOUVOU O VEDENÍ KONSORCIA A TĚMITO SMLUVNÍMI PODMÍNKAMI PŘEKROČIT DVOJNÁSOBEK POPLATKŮ SPLATNÝCH SPOLEČNOSTI ORCID PODLE SMLOUVY O VEDENÍ KONSORCIA BĚHEM POČÁTEČNÍHO OBDOBÍ NEBO AKTUÁLNÍHO PRODLOUŽENĚHO OBDOBÍ. STRANY (VČETNĚ JEJICH SPRÁVCŮ, ŘEDITELŮ, ÚŘEDNÍKŮ, ZAMĚSTNANCŮ, AGENTŮ, DODAVATELŮ A ZÁSTUPCŮ) V ŽÁDNÉM PŘÍPADĚ NENESOU ODPOVĚDNOST ZA JAKÉKOLI NEPŘÍMÉ, ZVLÁŠTNÍ, NÁSLEDNÉ NEBO SANKČNĚ NAHRAZOVANÉ ŠKODY. PRO VYLOUČENÍ POCHYBNOSTÍ SE ZA NEPŘÍMOU NEBO NÁSLEDNOU ŠKODU PRO ÚČELY PŘEDCHOZÍ VĚTY NEPOVAŽUJÍ JAKÉKOLI PLATBY VEDOUCÍHO KONSORCIA NEBO ČLENA KONSORCIA SPOLEČNOSTI ORCID V SOUVISLOSTI S NÁROKEM TŘETÍ STRANY VŮČI SPOLEČNOSTI ORCID.

6.3 Odpovědnost konsorcia. (i) *Vedoucí konsorcia* zajistí, aby každý Člen konsorcia byl plně seznámen s těmito Smluvními podmínkami, a podnikne přiměřeně kroky k zajištění toho, aby každý Člen konsorcia používal Registr ORCID a využíval Členské výhody v souladu s těmito Smluvními podmínkami. Vedoucí konsorcia je odpovědný za své vlastní jednání, opomenutí a narušení podle Smlouvy o vedení konsorcia a podle těchto Smluvních podmínek, mimo jiné včetně své povinnosti platit Poplatky podle Smlouvy o vedení konsorcia, svých povinností podle tohoto oddílu 6.3 (i) a svého prohlášení a záruky, že je oprávněn uzavřít tyto Smluvní podmínky. (ii) Každý *Člen konsorcia* je odpovědný za své vlastní jednání, opomenutí a narušení těchto Smluvních podmínek.

7. Platnost a ukončení smlouvy.

7.1 Období/prodlouženě období. Tyto Smluvní podmínky zůstávají v platnosti po dobu stanovenou ve Smlouvě o vedení konsorcia. Před koncem Počátečního období nebo Období obnovení poskytne ORCID Vedoucímu konsorcia oznámení o obnovení s uvedením data vypršení aktuálního období, data Období obnovení, příslušně poplatky za prodlouženě období, datum splatnosti těchto poplatků a Seznam členů konsorcia pro prodlouženě období. **Vedoucí konsorcia má 30 dní od data takového oznámení o prodloužení na to, aby (i) předložil společnosti ORCID protinávrh, pokud má v úmyslu neobnovit Smlouvu o vedení konsorcia, nebo (ii) poskytl společnosti ORCID aktualizovaný Seznam členů konsorcia pro prodloužení.** Každé prodlouženě období trvá termín stanovený v oznámení o obnovení a začíná prvním dnem po skončení Počátečního období nebo Prodlouženého období (pokud není v oznámení o prodloužení ze strany ORCID uvedeno jinak). **Prodloužení nevyžaduje podpis stran a má se za to, že k němu došlo, pokud Vedoucí konsorcia nepředloží v této 30denní lhůtě protinávrh na ukončení.** Poplatky a členství budou vycházet ze Složení konsorcia uvedeného v oznámení o prodloužení, pokud Vedoucí konsorcia včas nepředloží aktualizovaný Seznam členů konsorcia. Neuskutečnění včasné platby bez výjimky ze strany ORCID bude mít za následek automatické ukončení Smlouvy o vedení konsorcia na základě oznámení ze strany ORCID.

7.2 Ukončení bez udání důvodu. Společnost ORCID má právo ukončit Smlouvu o vedení konsorcia na konci Počátečního období nebo jakéhokoli Prodlouženého období výpovědí nejméně 60 dní před koncem aktuálního období. Vedoucí konsorcia může vypovědět Smlouvu o vedení konsorcia tím, že v reakci na oznámení o prodloužení poskytne společnosti ORCID protinávrh, jak je popsáno v oddíle 7.1.

7.3 Ukončení smlouvy z důvodu narušení. (i) *Ukončení z důvodu na straně Vedoucího konsorcia.* V případě, že se Vedoucí konsorcia domnívá, že společnost ORCID podstatně porušila jakékoli povinnosti, prohlášení nebo záruky podle Smlouvy o vedení konsorcia, písemně to oznámí společnosti ORCID. Společnost ORCID má 10 dnů od obdržení tohoto oznámení na nápravu údajného narušení a na písemné oznámení Vedoucímu konsorcia, že k nápravě došlo. Pokud nedojde k nápravě narušení v desetidenní lhůtě, má Vedoucí konsorcia právo na základě písemného oznámení okamžitě ukončit Smlouvu o vedení konsorcia. (ii) *Ukončení z důvodu na straně ORCID.* V případě, že se společnost ORCID domnívá, že Vedoucí konsorcia nebo Člen konsorcia podstatně porušil jakékoli povinnosti, prohlášení nebo záruky podle těchto Smluvních podmínek (nebo smlouvy o konsorciu v případě Vedoucího konsorcia), písemně to oznámí Vedoucímu konsorcia. Vedoucí konsorcia/Člen konsorcia má 10 dnů od obdržení tohoto oznámení na nápravu údajného narušení a na písemné oznámení (ORCIDU), že k nápravě došlo. Pokud nedojde k nápravě narušení během desetidenní lhůty, má ORCID právo tyto Smluvní podmínky ve vztahu k Členovi konsorcia okamžitě vypovědět na základě písemného oznámení; pokud je však stranou porušující smlouvu Vedoucí konsorcia, má ORCID právo vypovědět Smlouvu o vedení konsorcia jak ve vztahu k Vedoucímu konsorcia, tak ke každému Členu konsorcia. Žádné ustanovení tohoto oddílu 7.3 neomezuje práva společnosti ORCID podle oddílu 4.2.

7.4 Účinky ukončení. Po ukončení nebo vypršení platnosti těchto Smluvních podmínek (a/nebo Smlouvy o vedení konsorcia s ohledem na vedoucího konsorcia), podle toho, co nastane dříve, bude přístup k Členským

pověřením API a Členským výhodám pro každého Člena konsorcia okamžitě ukončen.
(a) *Ukončení činnosti konkrétního Člena.* Pokud se ukončení nebo vypršení platnosti týká pouze konkrétního Člena konsorcia (a nikoliv vedoucího konsorcia obecně), bude takový Člen konsorcia odstraněn z přílohy 1 Smlouvy o vedení konsorcia a bude ukončen pouze přístup takového Člena konsorcia k Členskému oprávnění API a k Členským výhodám. V rozsahu, v jakém Člen konsorcia uložil/upravil jakákoli Záznamová data, zůstanou tato Záznamová data v Registru ORCID, pokud je před ukončením neodstraní jednotlivec nebo určená Důvěryhodná osoba (určené Důvěryhodné osoby) a Důvěryhodné organizace nebo ORCID podle článku 5. Bez ohledu na výše uvedené má každý Člen konsorcia možnost opravit jakékoli informace, u nichž zjistí, že jsou nesprávné, po ukončení informováním ORCID, a ORCID se bude snažit nepřesnost neprodleně napravit u jednotlivce a/nebo prostřednictvím řešení sporů ORCID. V případě ukončení nebo vypršení platnosti konkrétního Člena konsorcia tyto Smluvní podmínky automaticky nezanikají ve vztahu k Vedoucímu konsorcia nebo ostatním Členům konsorcia. (b) *Ukončení činnosti Vedoucího konsorcia.* V případě ukončení nebo vypršení platnosti Vedoucího konsorcia má společnost ORCID možnost ukončit i práva každého Člena konsorcia podle této Smlouvy a v takovém případě umožní každému Členu konsorcia, který neporušil práva, uzavřít individuální členskou smlouvu pro členy ORCID přímo se společností ORCID za cenu pro individuální členy.
7.5 Pokračuiící platnost. Ustanovení oddílu 1.3 (ii) (Oprava záznamových údajů), oddílu 1.3 (iv) (Licence pro ORCID), oddílu 1.**8** (ii) (Použití údajů s omezeným přístupem), oddílu 1.9 (Omezení použití ORCID), oddílu 2.1 (Vlastnictví registru ORCID a označení), poslední věty oddílu 2.2 (používání ochranné známky ORCID), oddílu 5 (Postupy při řešení sporů), oddílu 6 (Obecná prohlášení a záruky, vyloučení odpovědnosti a omezení odpovědnosti), tohoto oddílu 7 (Doba platnosti a ukončení), oddílu **8** (Různé) a oddílu 9 (Definice) platí i po ukončení nebo vypršení platnosti Smlouvy o vedení konsorcia a těchto Smluvních podmínek.
8. Různé.
8.1 Úplnost smlouvy. Smlouva o vedení konsorcia, včetně těchto Smluvních podmínek a ustanovení, představuje úplnou dohodu mezi Vedoucím konsorcia a ORCID a nahrazuje jakákoli předchozí písemná nebo ústní ujednání s ohledem na její předmět. Tyto podmínky představují úplnou dohodu mezi ORCID a každým Členem konsorcia a nahrazují jakákoli předchozí ústní nebo písemná ujednání s ohledem na jejich předmět. Pokud strany uzavřely Standardní smluvní doložky související s předáváním a zpracováním osobních údajů, jsou tato ujednání rovněž nedílnou součástí smlouvy.
8.2 Úpravy smlouvy. Aby bylo možné zohlednit vývoj ORCID a jeho udržitelnost a fungovat v souladu se zákony v různých jurisdikcích, ORCID si vyhrazuje právo upravit tyto Smluvní podmínky za předpokladu, že (i) žádná taková úprava nebude mít zpětnou platnost; a (ii) ORCID poskytne vedoucímu konsorcia písemné oznámení 60 dní předem o jakýchkoli takových úpravách. Nový souhlas s těmito Smluvními podmínkami je podmínkou Členských výhod a licencí udělených podle těchto Smluvních podmínek. Pokud Vedoucí konsorcia vznese námitky proti jakýmkoli takovým úpravám, může Vedoucí konsorcia ukončit Smlouvu o vedení konsorcia (ke dni účinnosti takových změn) zasláním písemného oznámení ORCID před datem účinnosti a ORCID poskytne Vedoucímu konsorcia navrácení poměrné části poplatků. S výjimkou případů uvedených v této části **8**.2 nebo uvedených jinde v těchto Smluvních podmínkách (např. zvýšení Členských výhod, aktualizace kontaktních informací) a zde zahrnutých zásad (např. zásady ochrany osobních údajů, postupy pro řešení sporů ORCID), všechny dodatky Smlouvy o vedení konsorcia nebo jakákoli její část musí být vyhotoveny písemně a podepsány ORCID a Vedoucím konsorcia.
8.3 Oznámení. Veškerá oznámení, která ORCID vyžaduje podle Smlouvy o vedení konsorcia nebo jakékoli její části, se zasílají pouze hlavnímu kontaktu Vedoucího konsorcia. Je odpovědností Vedoucího konsorcia udržovat své kontaktní údaje aktuální a včas předat jakékoli takové oznámení každému Členovi konsorcia. Veškerá oznámení (ze strany ORCID nebo pro ORCID) podle Smlouvy o vedení konsorcia nebo stanov ORCID musí být písemná, v angličtině a zasílána následovně: (i) mezinárodně uznávaným kurýrem (např. FedEx, UPS) nebo (ii) elektronickou poštou. Oznámení se považuje za doručené a přijaté následující pracovní den po plánovaném datu doručení kurýrem a následující pracovní den po datu odeslání elektronickou poštou. ORCID nebo vedoucí konsorcia mohou průběžně změnit jméno a kontaktní informace ve Smlouvě o vedení konsorcia a v Seznamu členů konsorcia zasláním oznámení druhé straně v souladu s tímto oddílem.
8.4 Spory/rozhodné právo. Smlouva o vedení konsorcia nebo jakákoli její část je vykládána a řídí se zákony státu New York, Spojené státy americké, s výjimkou zákonů, které by mohly řídit aplikaci zákonů jiné jurisdikce. Použití Úmluvy Organizace spojených národů o smlouvách o mezinárodní koupi zboží je výslovně vyloučeno, je-li to relevantní. S výjimkou případů uvedených v postupech ORCID pro řešení sporů platí, že pokud strany nemohou vyřešit spory vyplývající ze Smlouvy o vedení konsorcia nebo s ní související smírnou cestou, učiní tak prostřednictvím rozhodčího řízení vedeného Americkou arbitrážní asociací v případě vnitrostátních sporů a Mezinárodním centrem pro řešení sporů Americké arbitrážní asociace v případě mezinárodních sporů (dále jen „AAA“), které se řídí jejími platnými pravidly, ve znění následujících ustanovení: (i) bez ohledu na výši sporné částky bude věc rozhodovat

jeden rozhodce znalý odvětví informačních technologií na základě písemných podání v angličtině a jednoho nebo více telefonických slyšení v angličtině (podle rozhodnutí rozhodce); (ii) strany předloží dokumenty týkající se rozhodčího řízení v souladu s pravidly AAA a podle pokynů rozhodce; a (iii) rozhodce vydá konečně závazně rozhodnutí 14 dní potě, co prohlásí slyšení za ukončeně. Rozsudek na základě nálezu vydaného rozhodcem může být vydán u kteréhokoli příslušného soudu. Bez ohledu na výše uvedené může kterákoli strana požádat rozhodce o soudní příkaz až do vydání rozhodčího nálezu nebo může, aniž by se vzdala jakéhokoli opravného prostředku podle Smlouvy o vedení konsorcia, požádat kterýkoli soud se sídlem v New Yorku, New York, Spojené státy americké (a ORCID, vedoucí konsorcia a každý Člen konsorcia s takovou jurisdikcí souhlasí) o soudní příkaz nebo jakýkoli jiný druh spravedlivého opatření, které je nezbytné k ochraně práv nebo majetku této strany, a to až do rozhodčího řízení nebo konečného rozhodnutí o podstatě sporu prostřednictvím rozhodčího řízení. Vedoucí konsorcia a Členové konsorcia berou na vědomí, že neoprávněné použití Členských oprávnění API, registru ORCID a/nebo narušení bezpečnosti může způsobit společnosti ORCID nenapravitelnou škodu.

8.5 Omezení postoupení. S výjimkou případů výslovně uvedených v tomto dokumentu nesmí žádná strana postoupit, uzavřít subdodavatelskou smlouvu nebo sublicencovat (souhrnně „převést“) svá práva a povinnosti vyplývající z jakékoliv části Smlouvy o vedení konsorcia, zcela nebo zčásti, bez předchozího písemného souhlasu Vedoucího konsorcia (v případě vedoucího konsorcia nebo člena konsorcia) nebo ORCID, pokud je to relevantní, a takový souhlas nebude bezdůvodně odmítnut, a jakýkoli opačný převod je neplatný; avšak za předpokladu, že převod ze strany ORCID (mimo jiné včetně převodu registru ORCID ze strany ORCID) v případě fúze, jiné restrukturalizace společnosti nebo zrušení společnosti je přípustný bez předchozího souhlasu za předpokladu, že (a) nabyvatel souhlasí s tím, že bude vázán podmínkami Smlouvy o vedení konsorcia, (b) oznámení je poskytnuto Vedoucímu konsorcia (v případě Vedoucího konsorcia nebo Člena konsorcia) a (c) takový nabyvatel je neziskový subjekt schopný plnit povinnosti ORCID podle této smlouvy a je v souladu s povinnostmi ORCID podle zásad ochrany osobních údajů.

8.6 Vyloučení zastoupení, společného podniku nebo partnerství. Nic z toho, co je obsaženo ve Smlouvě o vedení konsorcia, se nepovažuje za založení zastoupení, společného podniku nebo partnerství. (Bez ohledu na cokoli, co je v této smlouvě uvedeno jinak, nemají tyto Smluvní podmínky vliv na jakýkoli již existující vztah mezi Vedoucím konsorcia a Členem konsorcia.)

8.7 Neexistence oprávněných třetích stran. Smlouva o vedení konsorcia byla uzavřena výhradně ve prospěch ORCID, Vedoucího konsorcia a Členů konsorcia a není určena ve prospěch žádné třetí strany, bez ohledu na jakékoli zákony, které by tomu bránily.

8.8 Vzdání se nebo neplatnost jakéhokoli ustanovení. Vzdání se jakéhokoli ustanovení Smlouvy o vedení konsorcia nebude považováno za vzdání se jakéhokoli jiného jejího ustanovení, ani vzdání se jakéhokoli porušení jakékoli části Smlouvy o vedení konsorcia se nepovažuje za trvalé vzdání se dalších narušení stejných nebo jiných ustanovení. Pokud bude jakékoli ustanovení Smlouvy o vedení konsorcia považováno za neplatné, nezákonné, nevymahatelné nebo v rozporu se zákonem jakékoli jurisdikce, nebude tím nijak dotčena platnost, zákonnost a vymahatelnost zbývajících ustanovení.

8.9 Vyšší moc. Žádná ze stran neporušuje Smlouvu o vedení konsorcia, pokud nesplnění závazku podle této smlouvy vyplývá z podmínek, které jsou mimo přiměřenou kontrolu této strany, mimo jiné včetně stávek, pracovních sporů, teroristických činů nebo vládních požadavků.

8.10 Etické chování. Každá strana prohlašuje a zaručuje, že nejednala a nebude jednat, a pokud je jí známo, ani žádná osoba jednající jejím jménem, v rozporu s platnými zákony proti úplatkářství a korupci platnými v jurisdikci (jurisdikcích), kde působí, nebo s jejími vlastními interními zásadami týkajícími se těchto záležitostí. Bez ohledu na jakákoli jiná ustanovení této smlouvy může být jakékoli narušení tohoto oddílu jednou ze stran považováno druhou stranou za neschopné nápravy a umožňující straně, která se nedopustila narušení, okamžitě ukončit tyto Smluvní podmínky (nebo Smlouvu o vedení konsorcia s ohledem na vedoucího konsorcia a ORCID) na základě výpovědi bez újmy na jejích ostatních právech a opravných prostředcích.

8.11 Příprava návrhu. Tato smlouva nesmí být vykládána v neprospěch ORCID, jenž ji sepsal.

8.12 V případě jakýchkoliv nesrovnalostí nebo rozporů mezi anglickou a českou verzí této smlouvy má přednost anglická verze.

9. Definice

API nebo ORCID API: Viz členské rozhraní API níže.

Datum účinnosti konsorcia znamená datum účinnosti stanovené ve smlouvě o vedení konsorcia.

Smlouva o vedení konsorcia znamená (i) dokument nazvaný ORCID Consortium Lead Agreement, (ii) jeho přílohu **1** (ii) tyto Smluvní podmínky a (iv) výhody člena ORCID, zásady ochrany osobních údajů ORCID a postupy pro řešení sporů ORCID, které jsou začleněny odkazem v těchto podmínkách.

Složením konsorcia se rozumí počet členů konsorcia a výše poplatků každého člena.

Seznam členů konsorcia: Znamená seznam aktuálních členů konsorcia v online servisním nástroji ORCID, jak jej stanovil a aktualizoval vedoucí konsorcia a odsouhlasila společnost ORCID.

Datem účinnosti se u každého člena konsorcia rozumí datum, kdy vedoucí konsorcia přidá člena konsorcia na seznam členů konsorcia (se souhlasem ORCID). V případě vedoucího konsorcia se datem účinnosti rozumí datum

účinnosti konsorcia (jak je definováno ve smlouvé o vedení konsorcia).
Osobou se rozumí osoba, o níž existuje nebo se vytváří záznam ORCID.
Počátečním obdobím se rozumí doba trvání těchto Smluvních podmínek, jak je uvedeno ve smlouvé o konsorciu.
Data s omezeným přístupem jsou údaje o záznamech, které si prostřednictvím registru ORCID může zobrazit pouze jednotlivec, důvěryhodná osoba nebo určené důvěryhodné organizace.
Členem se rozumí jakákoli organizace, která uzavřela s ORCID Smluvní podmínky týkající se používání registru ORCID, členských oprávnění API a členských rozhraní API nebo jinak splňuje podmínky stanovené ORCID.
Členským oprávněním (oprávněními) API se rozumí jedinečný přístupový kód, který ORCID poskytuje každému členu konsorcia k používání členského API.
Členskými výhodami se rozumí využívání aspektů registru ORCID, které jsou k dispozici pouze členům ORCID, jak je popsáno v těchto Smluvních podmínkách a na internetových stránkách ORCID, ve znění občasných změn provedených společností ORCID.
Identifikátorem ORCID se rozumí globálně jedinečný identifikátor přidělený jednotlivci službou ORCID.
Postupy ORCID pro řešení sporů se rozumí postupy, které ORCID používá na pomoc členům a dalším uživatelům registru ORCID při řešení sporů o správnost údajů o záznamech, zveřejněné na webových stránkách ORCID na https://info.orcid.org/dispute-procedures/, ve znění občasných změn provedených ORCID.
Záznam ORCID znamená informace o jednotlivci v registru ORCID jiná než Systémové údaje.
Registrem ORCID se rozumí databáze ORCID, která obsahuje všechny údaje o záznamech.
Zásadami ochrany osobních údajů se rozumí postupy a závazky společnosti ORCID týkající se ochrany osobních údajů, které společnost ORCID zveřejňuje pod názvem „zásady ochrany osobních údajů“ na internetových stránkách ORCID na https://info.orcid.org/privacy-policy/, ve znění, které společnost ORCID čas od času mění.
Nastavení ochrany osobních údajů znamená volby určující, zda konkrétní údaje v rámci záznamu mají být *soukromými údaji*, *údaji s omezeným přístupem nebo veřejnými údaji*. (Další informace o nastavení ochrany osobních údajů naleznete v zásadách ochrany osobních údajů.)
Veřejné pověření API znamená jedinečný přístupový kód pro přístup k bezplatnému veřejnému API společnosti ORCID, které umožňuje jednotlivcům, kteří nejsou přidruženi k členům ORCID, připojit své systémy a aplikace k registru ORCID pomocí komunikace mezi stroji a číst veřejná data.
Veřejným datovým souborem se rozumí soubor všech veřejných dat v registru ORCID k danému datu, který lze stáhnout ze záznamů vytvořených nebo nárokovaných jednotlivcem.
Záznamovými daty se rozumí jednotlivé datové prvky v záznamu, včetně identifikátoru ORCID a metadat spojených s propojenými výzkumnými objekty. Za součást dat záznamu se považuje odkaz, nikoli však samotný odkazovaný objekt (např. text nebo úplná metadata).
Období obnovení znamená každé následující období následující po Počátečním období.
Systémovými údaji se rozumí údaje spojené se záznamem, které nejsou součástí viditelného registru ORCID, například heslo.
Smluvními podmínkami se rozumí tyto Podmínky členství v konsorciu ORCID.
Důvěryhodnou osobou se rozumí osoba, které jednotlivec udělil oprávnění spravovat záznam ORCID svým jménem, včetně nastavení soukromí, úprav a ukládání dat a jmenování důvěryhodných organizací.
Důvěryhodnou organizací se rozumí člen, kterému fyzická osoba (nebo její důvěryhodná osoba či osoby) udělila práva k ukládání
a upravování dat záznamu a/nebo čtení dat záznamu, která byla označena jako „data s omezeným přístupem“.
Použitím se rozumí použití, ukládání, poskytování sublicencí, reprodukce, úpravy, přenos, distribuce, veřejné předvádění a veřejné vystavování, včetně komerčního použití.

11. Příloha B – Standardní smluvní doložky (v originále Standard Contractual Clauses for the Transfer of Personal Data to Third Countries)

Příloha B obsahuje původní znění Standardni smluvní doložky v anglickém jazyce a následně i překlad do češtiny.

STANDARD CONTRACTUAL CLAUSES FOR THE TRANSFER OF PERSONAL DATA TO THIRD COUNTRIES
CONTROLLER TO CONTROLLER

WHEREAS, National Library of Technology ("Consortium Leader"), acting on its own behalf and as agent for each of its members identified by Consortium Leader in the ORCID self-service tool at http://orcid.org/self-service (as may be updated from time to time by Consortium Leader) (collectively, the "Consortium Members") and ORCID, Inc. ("ORCID") have entered into a Consortium Member License Agreement;
WHEREAS, in connection with such agreement, Consortium Leader and Consortium Members are transferring certain personal data to ORCID, and ORCID is processing such data;
WHEREAS, the European Commission has approved standard contractual clauses in the form set forth below for such transfer and processing of personal data;
WHEREAS, the Consortium Leader represents and warrants that it has the legal authority and has obtained legally permissible consents to act as the Consortium Members' agents and bind them to these standard contractual clauses;
WHEREAS, Consortium Leader and the Consortium Members are hereinafter referred to collectively as the 'data exporter' for purposes of Clause 1(b) below;
NOW THEREFORE, for good and valuable consideration, the sufficiency of which is acknowledged, the parties agree (i) on the following standard contractual clauses to ensure appropriate data protection safeguards for international data transfers and processing in connection with the Consortium Member License Agreement, and (ii) that Consortium Leader, Consortium Members and ORCID are hereby contractually bound by these standard contractual clauses.

SECTION I

Clause 1

Purpose and scope

(a) The purpose of these standard contractual clauses is to ensure compliance with the requirements of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) (1) for the transfer of personal data to a third country.

(b) The Parties:

  (i) the natural or legal person(s), public authority/ies, agency/ies or other body/ies (hereinafter 'entity/ies') transferring the personal data, as listed in Annex I.A and in the ORCID self-service tool at http://orcid.org/self-service (hereinafter each 'data exporter'), and

  (ii) the entity/ies in a third country receiving the personal data from the data exporter, directly or indirectly via another entity also Party to these Clauses, as listed in Annex I.A (hereinafter each 'data importer')

  have agreed to these standard contractual clauses (hereinafter: 'Clauses').

(c) These Clauses apply with respect to the transfer of personal data as specified in Annex I.B.

(d) The Appendix to these Clauses containing the Annexes referred to therein forms an integral part of these Clauses.

Clause 2

Effect and invariability of the Clauses

(a) These Clauses set out appropriate safeguards, including enforceable data subject rights and effective legal remedies, pursuant to Article 46(1) and Article 46(2)(c) of Regulation (EU) 2016/679 and, with respect to data transfers from controllers to processors and/or processors to processors, standard contractual clauses pursuant to Article 28(7) of Regulation (EU) 2016/679, provided they are not modified, except to select the appropriate Module(s) or to add or update information in the Appendix. This does not prevent the Parties from including the standard contractual clauses laid down in these Clauses in a wider contract and/or to add other clauses or additional safeguards, provided that they do not contradict, directly or indirectly, these Clauses or prejudice the fundamental rights or freedoms of data subjects.

(b) These Clauses are without prejudice to obligations to which the data exporter is subject by virtue of Regulation (EU) 2016/679.

Clause 3

Third-party beneficiaries

(a) Data subjects may invoke and enforce these Clauses, as third-party beneficiaries, against the data exporter and/or

data importer, with the following exceptions:

(i) Clause 1, Clause 2, Clause 3, Clause 6, Clause 7;
(ii) Clause 8.5 (e) and Clause 8.9(b);
(iii) Clause 12(a) and (d);
(iv) Clause 13;
(v) Clause 15.1(c), (d) and (e);
(vi) Clause 16(e);
(vii) Clause 18(a) and (b).

(b) Paragraph (a) is without prejudice to rights of data subjects under Regulation (EU) 2016/679.

Clause 4

Interpretation

(a) Where these Clauses use terms that are defined in Regulation (EU) 2016/679, those terms shall have the same meaning as in that Regulation.
(b) These Clauses shall be read and interpreted in the light of the provisions of Regulation (EU) 2016/679.
(c) These Clauses shall not be interpreted in a way that conflicts with rights and obligations provided for in Regulation (EU) 2016/679.

Clause 5

Hierarchy

In the event of a contradiction between these Clauses and the provisions of related agreements between the Parties, existing at the time these Clauses are agreed or entered into thereafter, these Clauses shall prevail.

Clause 6

Description of the transfer(s)

The details of the transfer(s), and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred, are specified in Annex I.B.

SECTION II – OBLIGATIONS OF THE PARTIES

Clause 8

Data protection safeguards

The data exporter warrants that it has used reasonable efforts to determine that the data importer is able, through the implementation of appropriate technical and organisational measures, to satisfy its obligations under these Clauses.

8.1 Purpose limitation

The data importer shall process the personal data only for the specific purpose(s) of the transfer, as set out in Annex I.B. It may only process the personal data for another purpose:

(i) where it has obtained the data subject's prior consent;
(ii) where necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings; or
(iii) where necessary in order to protect the vital interests of the data subject or of another natural person.

8.2 Transparency

(a) In order to enable data subjects to effectively exercise their rights pursuant to Clause 10, the data importer shall inform them, either directly or through the data exporter:
    (i) of its identity and contact details;
    (ii) of the categories of personal data processed;
    (iii) of the right to obtain a copy of these Clauses;
    (iv) where it intends to onward transfer the personal data to any third party/ies, of the recipient or categories of recipients (as appropriate with a view to providing meaningful information), the purpose of such onward transfer and the ground therefore pursuant to Clause 8.7.
(b) Paragraph (a) shall not apply where the data subject already has the information, including when such information has already been provided by the data exporter, or providing the information proves impossible or would involve a disproportionate effort for the data importer. In the latter case, the data importer shall, to the extent possible, make the information publicly available.

(c) On request, the Parties shall make a copy of these Clauses, including the Appendix as completed by them, available to the data subject free of charge. To the extent necessary to protect business secrets or other confidential information, including personal data, the Parties may redact part of the text of the Appendix prior to sharing a copy, but shall provide a meaningful summary where the data subject would otherwise not be able to understand its content or exercise his/her rights. On request, the Parties shall provide the data subject with the reasons for the redactions, to the extent possible without revealing the redacted information.

(d) Paragraphs (a) to (c) are without prejudice to the obligations of the data exporter under Articles 13 and 14 of Regulation (EU) 2016/679.

8.3 Accuracy and data minimisation

(a) Each Party shall ensure that the personal data is accurate and, where necessary, kept up to date. The data importer shall take every reasonable step to ensure that personal data that is inaccurate, having regard to the purpose(s) of processing, is erased or rectified without delay.

(b) If one of the Parties becomes aware that the personal data it has transferred or received is inaccurate, or has become outdated, it shall inform the other Party without undue delay.

(c) The data importer shall ensure that the personal data is adequate, relevant and limited to what is necessary in relation to the purpose(s) of processing.

8.4 Storage limitation

The data importer shall retain the personal data for no longer than necessary for the purpose(s) for which it is processed. It shall put in place appropriate technical or organisational measures to ensure compliance with this obligation, including erasure or anonymisation (2) of the data and all back-ups at the end of the retention period.

8.5 Security of processing

(a) The data importer and, during transmission, also the data exporter shall implement appropriate technical and organisational measures to ensure the security of the personal data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access (hereinafter 'personal data breach'). In assessing the appropriate level of security, they shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the data subject. The Parties shall in particular consider having recourse to encryption or pseudonymisation, including during transmission, where the purpose of processing can be fulfilled in that manner.

(b) The Parties have agreed on the technical and organisational measures set out in Annex II. The data importer shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security.

(c) The data importer shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

(d) In the event of a personal data breach concerning personal data processed by the data importer under these Clauses, the data importer shall take appropriate measures to address the personal data breach, including measures to mitigate its possible adverse effects.

(e) In case of a personal data breach that is likely to result in a risk to the rights and freedoms of natural persons, the data importer shall without undue delay notify both the data exporter and the competent supervisory authority pursuant to Clause 13. Such notification shall contain i) a description of the nature of the breach (including, where possible, categories and approximate number of data subjects and personal data records concerned), ii) its likely consequences, iii) the measures taken or proposed to address the breach, and iv) the details of a contact point from whom more information can be obtained. To the extent it is not possible for the data importer to provide all the information at the same time, it may do so in phases without undue further delay.

(f) In case of a personal data breach that is likely to result in a high risk to the rights and freedoms of natural persons, the data importer shall also notify without undue delay the data subjects concerned of the personal data breach and its nature, if necessary in cooperation with the data exporter, together with the information referred to in paragraph (e), points ii) to iv), unless the data importer has implemented measures to significantly reduce the risk to the rights or freedoms of natural persons, or notification would involve disproportionate efforts. In the latter case, the data importer shall instead issue a public communication or take a similar measure to inform the public of the personal data breach.

(g) The data importer shall document all relevant facts relating to the personal data breach, including its effects and any remedial action taken, and keep a record thereof.

8.6 Sensitive data

Where the transfer involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions or offences (hereinafter 'sensitive data'), the data importer shall apply specific restrictions and/or additional safeguards adapted to the specific nature of the data and the risks involved. This may include restricting the personnel permitted to access the personal data, additional security measures (such as pseudonymisation) and/or additional restrictions with respect to further disclosure.

8.7 Onward transfers

The data importer shall not disclose the personal data to a third party located outside the European Union (3) (in the same country as the data importer or in another third country, hereinafter 'onward transfer') unless the third party is or agrees to be bound by these Clauses, under the appropriate Module. Otherwise, an onward transfer by the data importer may only take place if:

(i) it is to a country benefiting from an adequacy decision pursuant to Article 45 of Regulation (EU) 2016/679 that covers the onward transfer;

(ii) the third party otherwise ensures appropriate safeguards pursuant to Articles 46 or 47 of Regulation (EU) 2016/679 with respect to the processing in question;

(iii) the third party enters into a binding instrument with the data importer ensuring the same level of data protection as under these Clauses, and the data importer provides a copy of these safeguards to the data exporter;

(iv) it is necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings;

(v) it is necessary in order to protect the vital interests of the data subject or of another natural person; or

(vi) where none of the other conditions apply, the data importer has obtained the explicit consent of the data subject for an onward transfer in a specific situation, after having informed him/her of its purpose(s), the identity of the recipient and the possible risks of such transfer to him/her due to the lack of appropriate data protection safeguards. In this case, the data importer shall inform the data exporter and, at the request of the latter, shall transmit to it a copy of the information provided to the data subject.

Any onward transfer is subject to compliance by the data importer with all the other safeguards under these Clauses, in particular purpose limitation.

Processing under the authority of the data importer

The data importer shall ensure that any person acting under its authority, including a processor, processes the data only on its instructions.

Documentation and compliance

(a) Each Party shall be able to demonstrate compliance with its obligations under these Clauses. In particular, the data importer shall keep appropriate documentation of the processing activities carried out under its responsibility.

(b) The data importer shall make such documentation available to the competent supervisory authority on request.

Clause 9 — Intentionally left blank

Clause 10

Data subject rights

(a) The data importer, where relevant with the assistance of the data exporter, shall deal with any enquiries and requests it receives from a data subject relating to the processing of his/her personal data and the exercise of his/her rights under these Clauses without undue delay and at the latest within one month of the receipt of the enquiry or request. (10) The data importer shall take appropriate measures to facilitate such enquiries, requests and the exercise of data subject rights. Any information provided to the data subject shall be in an intelligible and easily accessible form, using clear and plain language.

(b) In particular, upon request by the data subject the data importer shall, free of charge:

(i) provide confirmation to the data subject as to whether personal data concerning him/her is being processed and, where this is the case, a copy of the data relating to him/her and the information in Annex I; if personal data has been or will be onward transferred, provide information on recipients or categories of recipients (as appropriate with a view to providing meaningful information) to which the personal data

has been or will be onward transferred, the purpose of such onward transfers and their ground pursuant to Clause 8.7; and provide information on the right to lodge a complaint with a supervisory authority in accordance with Clause 12(c)(i);

(ii) rectify inaccurate or incomplete data concerning the data subject;

(iii) erase personal data concerning the data subject if such data is being or has been processed in violation of any of these Clauses ensuring third-party beneficiary rights, or if the data subject withdraws the consent on which the processing is based.

(c) Where the data importer processes the personal data for direct marketing purposes, it shall cease processing for such purposes if the data subject objects to it.

(d) The data importer shall not make a decision based solely on the automated processing of the personal data transferred (hereinafter 'automated decision'), which would produce legal effects concerning the data subject or similarly significantly affect him/her, unless with the explicit consent of the data subject or if authorised to do so under the laws of the country of destination, provided that such laws lays down suitable measures to safeguard the data subject's rights and legitimate interests. In this case, the data importer shall, where necessary in cooperation with the data exporter:

(i) inform the data subject about the envisaged automated decision, the envisaged consequences and the logic involved; and

(ii) implement suitable safeguards, at least by enabling the data subject to contest the decision, express his/her point of view and obtain review by a human being.

(e) Where requests from a data subject are excessive, in particular because of their repetitive character, the data importer may either charge a reasonable fee taking into account the administrative costs of granting the request or refuse to act on the request.

(f) The data importer may refuse a data subject's request if such refusal is allowed under the laws of the country of destination and is necessary and proportionate in a democratic society to protect one of the objectives listed in Article 23(1) of Regulation (EU) 2016/679.

(g) If the data importer intends to refuse a data subject's request, it shall inform the data subject of the reasons for the refusal and the possibility of lodging a complaint with the competent supervisory authority and/or seeking judicial redress.

Clause 11

Redress

(a) The data importer shall inform data subjects in a transparent and easily accessible format, through individual notice or on its website, of a contact point authorised to handle complaints. It shall deal promptly with any complaints it receives from a data subject.

(b) In case of a dispute between a data subject and one of the Parties as regards compliance with these Clauses, that Party shall use its best efforts to resolve the issue amicably in a timely fashion. The Parties shall keep each other informed about such disputes and, where appropriate, cooperate in resolving them.

(c) Where the data subject invokes a third-party beneficiary right pursuant to Clause 3, the data importer shall accept the decision of the data subject to:

(i) lodge a complaint with the supervisory authority in the Member State of his/her habitual residence or place of work, or the competent supervisory authority pursuant to Clause 13;

(ii) refer the dispute to the competent courts within the meaning of Clause 18.

(d) The Parties accept that the data subject may be represented by a not-for-profit body, organisation or association under the conditions set out in Article 80(1) of Regulation (EU) 2016/679.

(e) The data importer shall abide by a decision that is binding under the applicable EU or Member State law.

(f) The data importer agrees that the choice made by the data subject will not prejudice his/her substantive and procedural rights to seek remedies in accordance with applicable laws.

Clause 12

Liability

(a) Each Party shall be liable to the other Party/ies for any damages it causes the other Party/ies by any breach of these Clauses.

(b) Each Party shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages that the Party causes the data subject by breaching the third-party

beneficiary rights under these Clauses. This is without prejudice to the liability of the data exporter under Regulation (EU) 2016/679.

(c) Where more than one Party is responsible for any damage caused to the data subject as a result of a breach of these Clauses, all responsible Parties shall be jointly and severally liable and the data subject is entitled to bring an action in court against any of these Parties.

(d) The Parties agree that if one Party is held liable under paragraph (c), it shall be entitled to claim back from the other Party/ies that part of the compensation corresponding to its/their responsibility for the damage.

(e) The data importer may not invoke the conduct of a processor or sub-processor to avoid its own liability.

Clause 13

Supervision

(a) Where the data exporter is established in an EU Member State: The supervisory authority with responsibility for ensuring compliance by the data exporter with Regulation (EU) 2016/679 as regards the data transfer, as indicated in Annex I.C, shall act as competent supervisory authority.
Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) and has appointed a representative pursuant to Article 27(1) of Regulation (EU) 2016/679: The supervisory authority of the Member State in which the representative within the meaning of Article 27(1) of Regulation (EU) 2016/679 is established, as indicated in Annex I.C, shall act as competent supervisory authority.
Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) without however having to appoint a representative pursuant to Article 27(2) of Regulation (EU) 2016/679: The supervisory authority of one of the Member States in which the data subjects whose personal data is transferred under these Clauses in relation to the offering of goods or services to them, or whose behaviour is monitored, are located, as indicated in Annex I.C, shall act as competent supervisory authority.

(b) The data importer agrees to submit itself to the jurisdiction of and cooperate with the competent supervisory authority in any procedures aimed at ensuring compliance with these Clauses. In particular, the data importer agrees to respond to enquiries, submit to audits and comply with the measures adopted by the supervisory authority, including remedial and compensatory measures. It shall provide the supervisory authority with written confirmation that the necessary actions have been taken.

SECTION III – LOCAL LAWS AND OBLIGATIONS IN CASE OF ACCESS BY PUBLIC AUTHORITIES

Clause 14

Local laws and practices affecting compliance with the Clauses

(a) The Parties warrant that they have no reason to believe that the laws and practices in the third country of destination applicable to the processing of the personal data by the data importer, including any requirements to disclose personal data or measures authorising access by public authorities, prevent the data importer from fulfilling its obligations under these Clauses. This is based on the understanding that laws and practices that respect the essence of the fundamental rights and freedoms and do not exceed what is necessary and proportionate in a democratic society to safeguard one of the objectives listed in Article 23(1) of Regulation (EU) 2016/679, are not in contradiction with these Clauses.

(b) The Parties declare that in providing the warranty in paragraph (a), they have taken due account in particular of the following elements:

(i) the specific circumstances of the transfer, including the length of the processing chain, the number of actors involved and the transmission channels used; intended onward transfers; the type of recipient; the purpose of processing; the categories and format of the transferred personal data; the economic sector in which the transfer occurs; the storage location of the data transferred;

(ii) the laws and practices of the third country of destination– including those requiring the disclosure of data to public authorities or authorising access by such authorities – relevant in light of the specific circumstances of the transfer, and the applicable limitations and safeguards (12);

(iii) any relevant contractual, technical or organisational safeguards put in place to supplement the safeguards under these Clauses, including measures applied during transmission and to the processing of the personal data in the country of destination.

(c) The data importer warrants that, in carrying out the assessment under paragraph (b), it has made its best efforts to provide the data exporter with relevant information and agrees that it will continue to cooperate with the data exporter in ensuring compliance with these Clauses.

(d) The Parties agree to document the assessment under paragraph (b) and make it available to the competent supervisory authority on request.

(e) The data importer agrees to notify the data exporter promptly if, after having agreed to these Clauses and for the duration of the contract, it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under paragraph (a), including following a change in the laws of the third country or a measure (such as a disclosure request) indicating an application of such laws in practice that is not in line with the requirements in paragraph (a).

(f) Following a notification pursuant to paragraph (e), or if the data exporter otherwise has reason to believe that the data importer can no longer fulfil its obligations under these Clauses, the data exporter shall promptly identify appropriate measures (e.g. technical or organisational measures to ensure security and confidentiality) to be adopted by the data exporter and/or data importer to address the situation. The data exporter shall suspend the data transfer if it considers that no appropriate safeguards for such transfer can be ensured, or if instructed by the competent supervisory authority to do so. In this case, the data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses. If the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise. Where the contract is terminated pursuant to this Clause, Clause 16(d) and (e) shall apply.

Clause 15

Obligations of the data importer in case of access by public authorities

Notification

(a) The data importer agrees to notify the data exporter and, where possible, the data subject promptly (if necessary with the help of the data exporter) if it:

(i) receives a legally binding request from a public authority, including judicial authorities, under the laws of the country of destination for the disclosure of personal data transferred pursuant to these Clauses; such notification shall include information about the personal data requested, the requesting authority, the legal basis for the request and the response provided; or

(ii) becomes aware of any direct access by public authorities to personal data transferred pursuant to these Clauses in accordance with the laws of the country of destination; such notification shall include all information available to the importer.

(b) If the data importer is prohibited from notifying the data exporter and/or the data subject under the laws of the country of destination, the data importer agrees to use its best efforts to obtain a waiver of the prohibition, with a view to communicating as much information as possible, as soon as possible. The data importer agrees to document its best efforts in order to be able to demonstrate them on request of the data exporter.

(c) Where permissible under the laws of the country of destination, the data importer agrees to provide the data exporter, at regular intervals for the duration of the contract, with as much relevant information as possible on the requests received (in particular, number of requests, type of data requested, requesting authority/ies, whether requests have been challenged and the outcome of such challenges, etc.).

(d) The data importer agrees to preserve the information pursuant to paragraphs (a) to (c) for the duration of the contract and make it available to the competent supervisory authority on request.

(e) Paragraphs (a) to (c) are without prejudice to the obligation of the data importer pursuant to Clause 14(e) and Clause 16 to inform the data exporter promptly where it is unable to comply with these Clauses.

Review of legality and data minimisation

(f) The data importer agrees to review the legality of the request for disclosure, in particular whether it remains within the powers granted to the requesting public authority, and to challenge the request if, after careful assessment, it concludes that there are reasonable grounds to consider that the request is unlawful under the laws of the country of destination, applicable obligations under international law and principles of international comity. The data importer shall, under the same conditions, pursue possibilities of appeal. When challenging a request, the data importer shall seek interim measures with a view to suspending the effects of the request until the competent judicial authority has decided on its merits. It shall not disclose the personal data requested until required to do so under the applicable procedural rules. These requirements are without prejudice to the

obligations of the data importer under Clause 14(e).

(g) The data importer agrees to document its legal assessment and any challenge to the request for disclosure and, to the extent permissible under the laws of the country of destination, make the documentation available to the data exporter. It shall also make it available to the competent supervisory authority on request.

(h) The data importer agrees to provide the minimum amount of information permissible when responding to a request for disclosure, based on a reasonable interpretation of the request.

SECTION IV – FINAL PROVISIONS

Clause 16

Non-compliance with the Clauses and termination

(a) The data importer shall promptly inform the data exporter if it is unable to comply with these Clauses, for whatever reason.

(b) In the event that the data importer is in breach of these Clauses or unable to comply with these Clauses, the data exporter shall suspend the transfer of personal data to the data importer until compliance is again ensured or the contract is terminated. This is without prejudice to Clause 14(f).

(c) The data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses, where:

(i) the data exporter has suspended the transfer of personal data to the data importer pursuant to paragraph (b) and compliance with these Clauses is not restored within a reasonable time and in any event within one month of suspension;

(ii) the data importer is in substantial or persistent breach of these Clauses; or

(iii) the data importer fails to comply with a binding decision of a competent court or supervisory authority regarding its obligations under these Clauses.

In these cases, it shall inform the competent supervisory authority of such non-compliance. Where the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise.

(d) Personal data that has been transferred prior to the termination of the contract pursuant to paragraph (c) shall at the choice of the data exporter immediately be returned to the data exporter or deleted in its entirety. The same shall apply to any copies of the data. The data importer shall certify the deletion of the data to the data exporter. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit the return or deletion of the transferred personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process the data to the extent and for as long as required under that local law.

(e) Either Party may revoke its agreement to be bound by these Clauses where (i) the European Commission adopts a decision pursuant to Article 45(3) of Regulation (EU) 2016/679 that covers the transfer of personal data to which these Clauses apply; or (ii) Regulation (EU) 2016/679 becomes part of the legal framework of the country to which the personal data is transferred. This is without prejudice to other obligations applying to the processing in question under Regulation (EU) 2016/679.

Clause 17

Governing law

These Clauses shall be governed by the law of one of the EU Member States, provided such law allows for third-party beneficiary rights. The Parties agree that this shall be the law of Ireland.

Clause 18

Choice of forum and jurisdiction

(a) Any dispute arising from these Clauses shall be resolved by the courts of an EU Member State.

(b) The Parties agree that those shall be the courts of Ireland.

(c) A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of the Member State in which he/she has his/her habitual residence.

(d) The Parties agree to submit themselves to the jurisdiction of such courts.

ANNEX I

A. LIST OF PARTIES

Data exporter(s): *[Identity and contact details of the data exporter(s) and, where applicable, of its/their data protection officer and/or representative in the European Union].*

1. Name: .....
   Address: .....
   Contact person's name, position and contact details: .....
   .....
   Activities relevant to the data transferred under these Clauses: Using the ORCID Member API service to update records held on the ORCID Registry platform
   Signature and date:
   .....
   On behalf of itself and its Consortium Members.

Role (controller/processor): Controller.....

Data importer(s): *[Identity and contact details of the data importer(s), including any contact person with responsibility for data protection].*

1. Name: ORCID, Inc .....
   Address: 10411 Motor City Drive, Suite 750, Bethesda MD 20817, USA
   .....
   Contact person's name, position and contact details: Will Simpson; Director, Technology [redacted]
   .....
   Activities relevant to the data transferred under these Clauses: Providing the ORCID Member API service for updating records held on the ORCID Registry platform.
   Signature and date:
   ..... Role (controller/processor): Controller .....

B. DESCRIPTION OF TRANSFER

Categories of data subjects whose personal data is transferred

The personal data transferred may concern researchers, staff, students, grant applicants, grant applicant reviewers, authors, editors, journal reviewers, and other individuals involved in the activities of the exporter.

Categories of personal data transferred

- name (including variations of the data subject's name), email address, online and other social media profiles;
- details of grants and funding awarded or applied for by data subjects;
- details of research papers and other submissions (e.g. peer reviewed publications) or works developed or contributed to by data subjects;
- details of entities which the data subject is affiliated to or employed by;
- details of the data subject's education, qualifications, awards, honors, membership, service and positions (e.g. visiting fellow); and
- any other personal data that may be submitted to ORCID.

Sensitive data transferred (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialised training), keeping a record of access to the data, restrictions for onward transfers or additional security measures.

N/A

The frequency of the transfer (e.g., whether the data is transferred on a one-off or continuous basis).

The data will be transferred on a continuous basis, as determined by the exporter.

Nature of the processing

The personal data transferred will be subject to the following basic processing activities:

- Receiving data, including collection, accessing, retrieval, recording, and data entry
- Holding data, including storage, organisation and structuring

- Using data, including analysing, consultation, and testing
- Protecting data, including restricting, encrypting, and security testing
- Sharing data, including disclosure, dissemination, allowing access or otherwise making available
- Returning data to the data exporter or data subject
- Erasing data, including destruction and deletion

Purpose(s) of the data transfer and further processing
The transfer is made for the purpose of updating records held on the ORCID Registry platform.

The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period
The personal data will be retained for as long as required for the data importer to perform the services or as long as required to comply with applicable laws.
For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing
N/A

C. COMPETENT SUPERVISORY AUTHORITY

Identify the competent supervisory authority/ies in accordance with Clause 13
Data Protection Commission, Ireland

ANNEX II

TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

EXPLANATORY NOTE:

The technical and organizational measures must be described in specific (and not generic) terms. See also the general comment on the first page of the Appendix, in particular on the need to clearly indicate which measures apply to each transfer/set of transfers.

Description of the technical and organisational measures implemented by the data importer(s) (including any relevant certifications) to ensure an appropriate level of security, taking into account the nature, scope, context and purpose of the processing, and the risks for the rights and freedoms of natural persons.

1. **Security Policy and Procedures.** Data importer maintains a cybersecurity program that documents the policies, standards, and controls it uses that secure the information and resources related to the Services. The documentation includes organizational, administrative, technical, and physical safeguards and standards appropriate to the size and complexity, the scope of the activities, and the sensitivity of the Personal Data at issue
2. **Network Management.**
   a. **Event Logging.** Data importer has and will log all key security-related events, including user activities, exceptions, faults, and information security events, which will be produced, kept and regularly reviewed.
   b. **Remote Access.** Remote access to a network containing Personal Data or access to Customer systems will be done via a secure connection (e.g., VPN). All extranet connectivity into Customer systems will be through Customer-approved and authorized secure remote connections.
   c. **Access Control.** Data importer will restrict access to Personal Data to only authorized individuals. Data importer will regularly review user access privileges.
   d. **Network Controls.** Data importer will secure all data and communications networks to ensure the protection of Personal Data.
   e. **Malware Controls.** At all times during the provision of any Services, Data importer will make reasonable efforts to ensure that all Services do not contain malicious software or malware.
   f. **Encryption.** Data importer will encrypt all Personal Data in transit and at rest using industry standard encryption solutions.
   g. **Passwords and Multi-Factor Authentication.** Data importer personnel will use unique passwords that are regularly updated. All passwords must remain confidential and will not be shared between Data importer's employees, contractors, or third-party users. Data importer will implement multifactor authentication for accounts with access to Personal Data and Controller systems and networks.
   h. **Data Backups.** To ensure the ability to restore the availability and access to Personal Data in a timely manner in the event of a physical or technical incident, Data importer will ensure that backups of essential information and software, and in particular any Personal Data, are performed on a regular basis and Data importer shall test the backup process regularly.
3. **Physical Security.** Data importer will actively manage the physical security controls and ensure all buildings throughout Data importer's enterprise that house critical IT functions (e.g., data centers, network facilities, and key user areas) and store, process or transmit Personal Data are physically protected from unauthorized access.
4. **Training.** Data importer will provide training on data security and privacy matters so that all members of Data importer who handle Personal Data are trained in these matters.
5. **Information security incident management.** Data importer will maintain policies and procedures to develop a consistent and effective approach to the management of information security incidents.

STANDARD CONTRACTUAL CLAUSES FOR THE TRANSFER OF PERSONAL DATA TO THIRD COUNTRIES
CONTROLLER TO PROCESSOR

WHEREAS, National Library of Technology ("Consortium Leader"), acting on its own behalf and as agent for each of its members identified by Consortium Leader in the ORCID self-service tool at http://orcid.org/self-service (as may be updated from time to time by Consortium Leader) (collectively, the "Consortium Members") and ORCID, Inc. ("ORCID") have entered into a Consortium Member License Agreement;
WHEREAS, in connection with such agreement, Consortium Leader and Consortium Members are transferring certain personal data to ORCID, and ORCID is processing such data;
WHEREAS, the European Commission has approved standard contractual clauses in the form set forth below for such transfer and processing of personal data;
WHEREAS, the Consortium Leader represents and warrants that it has the legal authority and has obtained legally permissible consents to act as the Consortium Members' agents and bind them to these standard contractual clauses;
WHEREAS, Consortium Leader and the Consortium Members are hereinafter referred to collectively as the 'data exporter' for purposes of Clause 1(b) below)
NOW THEREFORE, for good and valuable consideration, the sufficiency of which is acknowledged, the parties agree (i) on the following standard contractual clauses to ensure appropriate data protection safeguards for international data transfers and processing and (ii) that Consortium Leader, Consortium Members and ORCID are hereby contractually bound by these standard contractual clauses.

SECTION I

Clause 1

Purpose and scope

(a) The purpose of these standard contractual clauses is to ensure compliance with the requirements of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) (1) for the transfer of personal data to a third country.

(b) The Parties:

(i) the natural or legal person(s), public authority/ies, agency/ies or other body/ies (hereinafter 'entity/ies') transferring the personal data, as listed in Annex I.A (hereinafter each 'data exporter'), and

(ii) the entity/ies in a third country receiving the personal data from the data exporter, directly or indirectly via another entity also Party to these Clauses, as listed in Annex I.A (hereinafter each 'data importer')

have agreed to these standard contractual clauses (hereinafter: 'Clauses').

(c) These Clauses apply with respect to the transfer of personal data as specified in Annex I.B.

(d) The Appendix to these Clauses containing the Annexes referred to therein forms an integral part of these Clauses.

Clause 2

Effect and invariability of the Clauses

(a) These Clauses set out appropriate safeguards, including enforceable data subject rights and effective legal remedies, pursuant to Article 46(1) and Article 46(2)(c) of Regulation (EU) 2016/679 and, with respect to data transfers from controllers to processors and/or processors to processors, standard contractual clauses pursuant to Article 28(7) of Regulation (EU) 2016/679, provided they are not modified, except to select the appropriate Module(s) or to add or update information in the Appendix. This does not prevent the Parties from including the standard contractual clauses laid down in these Clauses in a wider contract and/or to add other clauses or additional safeguards, provided that they do not contradict, directly or indirectly, these Clauses or prejudice the fundamental rights or freedoms of data subjects.

(b) These Clauses are without prejudice to obligations to which the data exporter is subject by virtue of Regulation (EU) 2016/679.

Clause 3

Third-party beneficiaries

(a) Data subjects may invoke and enforce these Clauses, as third-party beneficiaries, against the data exporter and/or data importer, with the following exceptions:
   (i) Clause 1, Clause 2, Clause 3, Clause 6, Clause 7;
   (ii) Clause 8.1(b), 8.9(a), (c), (d) and (e);
   (iii) Clause 9(a), (c), (d) and (e);
   (iv) Clause 12(a), (d) and (f);
   (v) Clause 13;
   (vi) Clause 15.1(c), (d) and (e);
   (vii) Clause 16(e);
   (viii) Clause 18(a) and (b).
(b) Paragraph (a) is without prejudice to rights of data subjects under Regulation (EU) 2016/679.

Clause 4

Interpretation

(a) Where these Clauses use terms that are defined in Regulation (EU) 2016/679, those terms shall have the same meaning as in that Regulation.
(b) These Clauses shall be read and interpreted in the light of the provisions of Regulation (EU) 2016/679.
(c) These Clauses shall not be interpreted in a way that conflicts with rights and obligations provided for in Regulation (EU) 2016/679.

Clause 5

Hierarchy

In the event of a contradiction between these Clauses and the provisions of related agreements between the Parties, existing at the time these Clauses are agreed or entered into thereafter, these Clauses shall prevail.

Clause 6

Description of the transfer(s)

The details of the transfer(s), and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred, are specified in Annex I.B.

SECTION II – OBLIGATIONS OF THE PARTIES

Clause 8

Data protection safeguards

The data exporter warrants that it has used reasonable efforts to determine that the data importer is able, through the implementation of appropriate technical and organisational measures, to satisfy its obligations under these Clauses.

8.1 Instructions

(a) The data importer shall process the personal data only on documented instructions from the data exporter. The data exporter may give such instructions throughout the duration of the contract.
(b) The data importer shall immediately inform the data exporter if it is unable to follow those instructions.

8.2 Purpose limitation

The data importer shall process the personal data only for the specific purpose(s) of the transfer, as set out in Annex I.B, unless on further instructions from the data exporter.

8.3 Transparency

On request, the data exporter shall make a copy of these Clauses, including the Appendix as completed by the Parties, available to the data subject free of charge. To the extent necessary to protect business secrets or other confidential information, including the measures described in Annex II and personal data, the data exporter may redact part of the text of the Appendix to these Clauses prior to sharing a copy, but shall provide a meaningful summary where the data subject would otherwise not be able to understand its content or exercise his/her rights. On request, the Parties shall provide the data subject with the reasons for the redactions, to the extent possible without revealing the redacted information. This Clause is without prejudice to the obligations of the data exporter under Articles 13 and 14 of Regulation (EU) 2016/679.

8.4 Accuracy

If the data importer becomes aware that the personal data it has received is inaccurate, or has become outdated, it shall inform the data exporter without undue delay. In this case, the data importer shall cooperate with the data exporter to erase or rectify the data.

8.5 Duration of processing and erasure or return of data

Processing by the data importer shall only take place for the duration specified in Annex I.B. After the end of the provision of the processing services, the data importer shall, at the choice of the data exporter, delete all personal data processed on behalf of the data exporter and certify to the data exporter that it has done so, or return to the data exporter all personal data processed on its behalf and delete existing copies. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit return or deletion of the personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process it to the extent and for as long as required under that local law. This is without prejudice to Clause 14, in particular the requirement for the data importer under Clause 14(e) to notify the data exporter throughout the duration of the contract if it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under Clause 14(a).

8.6 Security of processing

(a) The data importer and, during transmission, also the data exporter shall implement appropriate technical and organisational measures to ensure the security of the data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to that data (hereinafter 'personal data breach'). In assessing the appropriate level of security, the Parties shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the data subjects. The Parties shall in particular consider having recourse to encryption or pseudonymisation, including during transmission, where the purpose of processing can be fulfilled in that manner. In case of pseudonymisation, the additional information for attributing the personal data to a specific data subject shall, where possible, remain under the exclusive control of the data exporter. In complying with its obligations under this paragraph, the data importer shall at least implement the technical and organisational measures specified in Annex II. The data importer shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security.

(b) The data importer shall grant access to the personal data to members of its personnel only to the extent strictly necessary for the implementation, management and monitoring of the contract. It shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

(c) In the event of a personal data breach concerning personal data processed by the data importer under these Clauses, the data importer shall take appropriate measures to address the breach, including measures to mitigate its adverse effects. The data importer shall also notify the data exporter without undue delay after having become aware of the breach. Such notification shall contain the details of a contact point where more information can be obtained, a description of the nature of the breach (including, where possible, categories and approximate number of data subjects and personal data records concerned), its likely consequences and the measures taken or proposed to address the breach including, where appropriate, measures to mitigate its possible adverse effects. Where, and in so far as, it is not possible to provide all information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

(d) The data importer shall cooperate with and assist the data exporter to enable the data exporter to comply with its obligations under Regulation (EU) 2016/679, in particular to notify the competent supervisory authority and the affected data subjects, taking into account the nature of processing and the information available to the data importer.

8.7 Sensitive data

Where the transfer involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions and offences (hereinafter 'sensitive data'), the data importer shall apply the specific restrictions and/or additional safeguards described in Annex I.B.

8.8 Onward transfers

The data importer shall only disclose the personal data to a third party on documented instructions from the data exporter. In addition, the data may only be disclosed to a third party located outside the European Union (4) (in the same country as the data importer or in another third country, hereinafter 'onward transfer') if the third party is or agrees to be bound by these Clauses, under the appropriate Module, or if:

(i) the onward transfer is to a country benefiting from an adequacy decision pursuant to Article 45 of Regulation (EU) 2016/679 that covers the onward transfer;

(ii) the third party otherwise ensures appropriate safeguards pursuant to Articles 46 or 47 Regulation of (EU) 2016/679 with respect to the processing in question;

(iii) the onward transfer is necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings; or

(iv) the onward transfer is necessary in order to protect the vital interests of the data subject or of another natural person.

Any onward transfer is subject to compliance by the data importer with all the other safeguards under these Clauses, in particular purpose limitation.

8.9 Documentation and compliance

(a) The data importer shall promptly and adequately deal with enquiries from the data exporter that relate to the processing under these Clauses.

(b) The Parties shall be able to demonstrate compliance with these Clauses. In particular, the data importer shall keep appropriate documentation on the processing activities carried out on behalf of the data exporter.

(c) The data importer shall make available to the data exporter all information necessary to demonstrate compliance with the obligations set out in these Clauses and at the data exporter's request, allow for and contribute to audits of the processing activities covered by these Clauses, at reasonable intervals or if there are indications of non-compliance. In deciding on a review or audit, the data exporter may take into account relevant certifications held by the data importer.

(d) The data exporter may choose to conduct the audit by itself or mandate an independent auditor. Audits may include inspections at the premises or physical facilities of the data importer and shall, where appropriate, be carried out with reasonable notice.

(e) The Parties shall make the information referred to in paragraphs (b) and (c), including the results of any audits, available to the competent supervisory authority on request.

Clause 9

Use of sub-processors

The data importer has the data exporter's general authorisation for the engagement of sub-processor(s) from an agreed list. The data importer shall specifically inform the data exporter in writing of any intended changes to that list through the addition or replacement of sub-processors at least thirty days in advance, thereby giving the data exporter sufficient time to be able to object to such changes prior to the engagement of the sub-processor(s). The data importer shall provide the data exporter with the information necessary to enable the data exporter to exercise its right to object.

(a) Where the data importer engages a sub-processor to carry out specific processing activities (on behalf of the data exporter), it shall do so by way of a written contract that provides for, in substance, the same data protection obligations as those binding the data importer under these Clauses, including in terms of third-party beneficiary rights for data subjects. (8) The Parties agree that, by complying with this Clause, the data importer fulfils its obligations under Clause 8.8. The data importer shall ensure that the sub-processor complies with the obligations to which the data importer is subject pursuant to these Clauses.

(b) The data importer shall provide, at the data exporter's request, a copy of such a sub-processor agreement and any subsequent amendments to the data exporter. To the extent necessary to protect business secrets or other confidential information, including personal data, the data importer may redact the text of the agreement prior to sharing a copy.

(c) The data importer shall remain fully responsible to the data exporter for the performance of the sub-processor's obligations under its contract with the data importer. The data importer shall notify the data exporter of any failure by the sub-processor to fulfil its obligations under that contract.

(d) The data importer shall agree a third-party beneficiary clause with the sub-processor whereby – in the event the data importer has factually disappeared, ceased to exist in law or has become insolvent – the data exporter shall have the

right to terminate the sub-processor contract and to instruct the sub-processor to erase or return the personal data.

Clause 10

Data subject rights

(a) The data importer shall promptly notify the data exporter of any request it has received from a data subject. It shall not respond to that request itself unless it has been authorised to do so by the data exporter.

(b) The data importer shall assist the data exporter in fulfilling its obligations to respond to data subjects' requests for the exercise of their rights under Regulation (EU) 2016/679. In this regard, the Parties shall set out in Annex II the appropriate technical and organisational measures, taking into account the nature of the processing, by which the assistance shall be provided, as well as the scope and the extent of the assistance required.

(c) In fulfilling its obligations under paragraphs (a) and (b), the data importer shall comply with the instructions from the data exporter.

Clause 11

Redress

(a) The data importer shall inform data subjects in a transparent and easily accessible format, through individual notice or on its website, of a contact point authorised to handle complaints. It shall deal promptly with any complaints it receives from a data subject.

(b) In case of a dispute between a data subject and one of the Parties as regards compliance with these Clauses, that Party shall use its best efforts to resolve the issue amicably in a timely fashion. The Parties shall keep each other informed about such disputes and, where appropriate, cooperate in resolving them.

(c) Where the data subject invokes a third-party beneficiary right pursuant to Clause 3, the data importer shall accept the decision of the data subject to:

   (i) lodge a complaint with the supervisory authority in the Member State of his/her habitual residence or place of work, or the competent supervisory authority pursuant to Clause 13;

   (ii) refer the dispute to the competent courts within the meaning of Clause 18.

(d) The Parties accept that the data subject may be represented by a not-for-profit body, organisation or association under the conditions set out in Article 80(1) of Regulation (EU) 2016/679.

(e) The data importer shall abide by a decision that is binding under the applicable EU or Member State law.

(f) The data importer agrees that the choice made by the data subject will not prejudice his/her substantive and procedural rights to seek remedies in accordance with applicable laws.

Clause 12

Liability

(a) Each Party shall be liable to the other Party/ies for any damages it causes the other Party/ies by any breach of these Clauses.

(b) The data importer shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data importer or its sub-processor causes the data subject by breaching the third-party beneficiary rights under these Clauses.

(c) Notwithstanding paragraph (b), the data exporter shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data exporter or the data importer (or its sub-processor) causes the data subject by breaching the third-party beneficiary rights under these Clauses. This is without prejudice to the liability of the data exporter and, where the data exporter is a processor acting on behalf of a controller, to the liability of the controller under Regulation (EU) 2016/679 or Regulation (EU) 2018/1725, as applicable.

(d) The Parties agree that if the data exporter is held liable under paragraph (c) for damages caused by the data importer (or its sub-processor), it shall be entitled to claim back from the data importer that part of the compensation corresponding to the data importer's responsibility for the damage.

(e) Where more than one Party is responsible for any damage caused to the data subject as a result of a breach of these Clauses, all responsible Parties shall be jointly and severally liable and the data subject is entitled to bring an action in court against any of these Parties.

(f) The Parties agree that if one Party is held liable under paragraph (e), it shall be entitled to claim back from the

other Party/ies that part of the compensation corresponding to its/their responsibility for the damage.

(g) The data importer may not invoke the conduct of a sub-processor to avoid its own liability.

Clause 13

Supervision

(a) Where the data exporter is established in an EU Member State: The supervisory authority with responsibility for ensuring compliance by the data exporter with Regulation (EU) 2016/679 as regards the data transfer, as indicated in Annex I.C, shall act as competent supervisory authority.

Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) and has appointed a representative pursuant to Article 27(1) of Regulation (EU) 2016/679: The supervisory authority of the Member State in which the representative within the meaning of Article 27(1) of Regulation (EU) 2016/679 is established, as indicated in Annex I.C, shall act as competent supervisory authority.

Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) without however having to appoint a representative pursuant to Article 27(2) of Regulation (EU) 2016/679: The supervisory authority of one of the Member States in which the data subjects whose personal data is transferred under these Clauses in relation to the offering of goods or services to them, or whose behaviour is monitored, are located, as indicated in Annex I.C, shall act as competent supervisory authority.

(b) The data importer agrees to submit itself to the jurisdiction of and cooperate with the competent supervisory authority in any procedures aimed at ensuring compliance with these Clauses. In particular, the data importer agrees to respond to enquiries, submit to audits and comply with the measures adopted by the supervisory authority, including remedial and compensatory measures. It shall provide the supervisory authority with written confirmation that the necessary actions have been taken.

SECTION III – LOCAL LAWS AND OBLIGATIONS IN CASE OF ACCESS BY PUBLIC AUTHORITIES

Clause 14

Local laws and practices affecting compliance with the Clauses

(a) The Parties warrant that they have no reason to believe that the laws and practices in the third country of destination applicable to the processing of the personal data by the data importer, including any requirements to disclose personal data or measures authorising access by public authorities, prevent the data importer from fulfilling its obligations under these Clauses. This is based on the understanding that laws and practices that respect the essence of the fundamental rights and freedoms and do not exceed what is necessary and proportionate in a democratic society to safeguard one of the objectives listed in Article 23(1) of Regulation (EU) 2016/679, are not in contradiction with these Clauses.

(b) The Parties declare that in providing the warranty in paragraph (a), they have taken due account in particular of the following elements:

(i) the specific circumstances of the transfer, including the length of the processing chain, the number of actors involved and the transmission channels used; intended onward transfers; the type of recipient; the purpose of processing; the categories and format of the transferred personal data; the economic sector in which the transfer occurs; the storage location of the data transferred;

(ii) the laws and practices of the third country of destination– including those requiring the disclosure of data to public authorities or authorising access by such authorities – relevant in light of the specific circumstances of the transfer, and the applicable limitations and safeguards (12);

(iii) any relevant contractual, technical or organisational safeguards put in place to supplement the safeguards under these Clauses, including measures applied during transmission and to the processing of the personal data in the country of destination.

(c) The data importer warrants that, in carrying out the assessment under paragraph (b), it has made its best efforts to provide the data exporter with relevant information and agrees that it will continue to cooperate with the data exporter in ensuring compliance with these Clauses.

(d) The Parties agree to document the assessment under paragraph (b) and make it available to the competent

supervisory authority on request.

(e) The data importer agrees to notify the data exporter promptly if, after having agreed to these Clauses and for the duration of the contract, it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under paragraph (a), including following a change in the laws of the third country or a measure (such as a disclosure request) indicating an application of such laws in practice that is not in line with the requirements in paragraph (a).

(f) Following a notification pursuant to paragraph (e), or if the data exporter otherwise has reason to believe that the data importer can no longer fulfil its obligations under these Clauses, the data exporter shall promptly identify appropriate measures (e.g. technical or organisational measures to ensure security and confidentiality) to be adopted by the data exporter and/or data importer to address the situation. The data exporter shall suspend the data transfer if it considers that no appropriate safeguards for such transfer can be ensured, or if instructed by the competent supervisory authority to do so. In this case, the data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses. If the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise. Where the contract is terminated pursuant to this Clause, Clause 16(d) and (e) shall apply.

Clause 15

Obligations of the data importer in case of access by public authorities

15.1 Notification

(a) The data importer agrees to notify the data exporter and, where possible, the data subject promptly (if necessary with the help of the data exporter) if it:

  (i) receives a legally binding request from a public authority, including judicial authorities, under the laws of the country of destination for the disclosure of personal data transferred pursuant to these Clauses; such notification shall include information about the personal data requested, the requesting authority, the legal basis for the request and the response provided; or

  (ii) becomes aware of any direct access by public authorities to personal data transferred pursuant to these Clauses in accordance with the laws of the country of destination; such notification shall include all information available to the importer.

(b) If the data importer is prohibited from notifying the data exporter and/or the data subject under the laws of the country of destination, the data importer agrees to use its best efforts to obtain a waiver of the prohibition, with a view to communicating as much information as possible, as soon as possible. The data importer agrees to document its best efforts in order to be able to demonstrate them on request of the data exporter.

(c) Where permissible under the laws of the country of destination, the data importer agrees to provide the data exporter, at regular intervals for the duration of the contract, with as much relevant information as possible on the requests received (in particular, number of requests, type of data requested, requesting authority/ies, whether requests have been challenged and the outcome of such challenges, etc.).

(d) The data importer agrees to preserve the information pursuant to paragraphs (a) to (c) for the duration of the contract and make it available to the competent supervisory authority on request.

(e) Paragraphs (a) to (c) are without prejudice to the obligation of the data importer pursuant to Clause 14(e) and Clause 16 to inform the data exporter promptly where it is unable to comply with these Clauses.

15.2 Review of legality and data minimisation

(a) The data importer agrees to review the legality of the request for disclosure, in particular whether it remains within the powers granted to the requesting public authority, and to challenge the request if, after careful assessment, it concludes that there are reasonable grounds to consider that the request is unlawful under the laws of the country of destination, applicable obligations under international law and principles of international comity. The data importer shall, under the same conditions, pursue possibilities of appeal. When challenging a request, the data importer shall seek interim measures with a view to suspending the effects of the request until the competent judicial authority has decided on its merits. It shall not disclose the personal data requested until required to do so under the applicable procedural rules. These requirements are without prejudice to the obligations of the data importer under Clause 14(e).

(b) The data importer agrees to document its legal assessment and any challenge to the request for disclosure

and, to the extent permissible under the laws of the country of destination, make the documentation available to the data exporter. It shall also make it available to the competent supervisory authority on request.

(c) The data importer agrees to provide the minimum amount of information permissible when responding to a request for disclosure, based on a reasonable interpretation of the request.

SECTION IV – FINAL PROVISIONS

Clause 16

Non-compliance with the Clauses and termination

(a) The data importer shall promptly inform the data exporter if it is unable to comply with these Clauses, for whatever reason.

(b) In the event that the data importer is in breach of these Clauses or unable to comply with these Clauses, the data exporter shall suspend the transfer of personal data to the data importer until compliance is again ensured or the contract is terminated. This is without prejudice to Clause 14(f).

(c) The data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses, where:

(i) the data exporter has suspended the transfer of personal data to the data importer pursuant to paragraph (b) and compliance with these Clauses is not restored within a reasonable time and in any event within one month of suspension;

(ii) the data importer is in substantial or persistent breach of these Clauses; or

(iii) the data importer fails to comply with a binding decision of a competent court or supervisory authority regarding its obligations under these Clauses.

In these cases, it shall inform the competent supervisory authority of such non-compliance. Where the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise.

(d) Personal data that has been transferred prior to the termination of the contract pursuant to paragraph (c) shall at the choice of the data exporter immediately be returned to the data exporter or deleted in its entirety. The same shall apply to any copies of the data. The data importer shall certify the deletion of the data to the data exporter. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit the return or deletion of the transferred personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process the data to the extent and for as long as required under that local law.

(e) Either Party may revoke its agreement to be bound by these Clauses where (i) the European Commission adopts a decision pursuant to Article 45(3) of Regulation (EU) 2016/679 that covers the transfer of personal data to which these Clauses apply; or (ii) Regulation (EU) 2016/679 becomes part of the legal framework of the country to which the personal data is transferred. This is without prejudice to other obligations applying to the processing in question under Regulation (EU) 2016/679.

Clause 17

Governing law

These Clauses shall be governed by the law of the EU Member State in which the data exporter is established. Where such law does not allow for third-party beneficiary rights, they shall be governed by the law of another EU Member State that does allow for third-party beneficiary rights. The Parties agree that this shall be the law of Ireland

Clause 18

Choice of forum and jurisdiction

(a) Any dispute arising from these Clauses shall be resolved by the courts of an EU Member State.

(b) The Parties agree that those shall be the courts of Ireland.

(c) A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of the Member State in which he/she has his/her habitual residence.

(d) The Parties agree to submit themselves to the jurisdiction of such courts.

ANNEX I

A. LIST OF PARTIES

Data exporter(s): *(Identity and contact details of the data exporter(s) and, where applicable, of its/their data protection officer and/or representative in the European Union).*

1. Name: ……

Address: ……

Contact person's name, position and contact details: ……

……

Activities relevant to the data transferred under these Clauses: Using the service provided to enable management of the exporter's ORCID membership, and tools for updating records held on the ORCID Registry platform

……

Signature and date:

…… Role (controller/processor): Controller

……

On behalf of itself and its Consortium Members.

Data importer(s): *(Identity and contact details of the data importer(s), including any contact person with responsibility for data protection).*

1. Name: ORCID, Inc ……

Address: 10411 Motor City Drive, Suite 750, Bethesda MD 20817, USA

……

Contact person's name, position and contact details: Will Simpson; Director, Technology; [redacted]

……

Activities relevant to the data transferred under these Clauses: Providing a service to the importer to enable management of itsr ORCID membership, and tools for updating records held on the ORCID Registry platform

……

Signature and date:

……

Role (controller/processor): Processor ……

B. DESCRIPTION OF TRANSFER

Categories of data subjects whose personal data is transferred

The personal data transferred may concern researchers, staff, students, grant applicants, grant applicant reviewers, authors, editors, journal reviewers, and other individuals involved in the activities of the exporter.

Categories of personal data transferred

- name (including variations of the data subject's name), email address, online and other social media profiles
- details of grants and funding awarded or applied for by data subjects
- details of researcher papers and other submissions (e.g. peer reviewed publications) or works developed or contributed to by data subjects
- details of entities which the data subject is affiliated to or employed by
- details of the data subject's education, qualifications, awards, honors, membership, service and positions (e.g. visiting fellow)
- any other personal data that may be submitted to ORCID

Sensitive data transferred (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialised training), keeping a record of access to the data, restrictions for onward transfers or additional security measures.

N/A

The frequency of the transfer (e.g., whether the data is transferred on a one-off or continuous basis)

The data will be transferred on a continuous basis, as determined by the exporter.

Nature of the processing

The personal data transferred will be subject to the following basic processing activities:

- Receiving data, including collection, accessing, retrieval, recording, and data entry
- Holding data, including storage, organisation and structuring
- Using data, including analysing, consultation, and testing
- Protecting data, including restricting, encrypting, and security testing
- Sharing data, including disclosure, dissemination, allowing access or otherwise making available
- Returning data to the data exporter or data subject
- Erasing data, including destruction and deletion

Purpose(s) of the data transfer and further processing

Providing a service to the importer to enable management of its ORCID membership, and tools for updating records held on the ORCID Registry platform.

The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period.

The personal data will be retained for as long as required for the data importer to perform the services or as long as required to comply with applicable laws.

For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing

The subject matter, nature, and duration of the processing of Personal Data is as described above.

C. COMPETENT SUPERVISORY AUTHORITY

Identify the competent supervisory authority/ies in accordance with Clause 13

Data Protection Commission, Ireland .....

ANNEX II

TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

Description of the technical and organisational measures implemented by the data importer(s) (including any relevant certifications) to ensure an appropriate level of security, taking into account the nature, scope, context and purpose of the processing, and the risks for the rights and freedoms of natural persons.

1. **Security Policy and Procedures.** Data importer maintains a cybersecurity program that documents the policies, standards, and controls it uses that secure the information and resources related to the Services. The documentation includes organizational, administrative, technical, and physical safeguards and standards appropriate to the size and complexity, the scope of the activities, and the sensitivity of the Personal Data at issue
2. **Network Management.**
    a. **Event Logging.** Data importer has and will log all key security-related events, including user activities, exceptions, faults, and information security events, which will be produced, kept and regularly reviewed.
    b. **Remote Access.** Remote access to a network containing Personal Data or access to Customer systems will be done via a secure connection (e.g., VPN). All extranet connectivity into Customer systems will be through Customer-approved and authorized secure remote connections.
    c. **Access Control.** Data importer will restrict access to Personal Data to only authorized individuals. Data importer will regularly review user access privileges.
    d. **Network Controls.** Data importer will secure all data and communications networks to ensure the protection of Personal Data.
    e. **Malware Controls.** At all times during the provision of any Services, Data importer will make reasonable efforts to ensure that all Services do not contain malicious software or malware.
    f. **Encryption.** Data importer will encrypt all Personal Data in transit and at rest using industry standard encryption solutions.
    g. **Passwords and Multi-Factor Authentication.** Data importer personnel will use unique passwords that are regularly updated. All passwords must remain confidential and will not be shared between Data importer's employees, contractors, or third-party users. Data importer will implement multifactor authentication for accounts with access to Personal Data and Controller systems and networks.
    h. **Data Backups.** To ensure the ability to restore the availability and access to Personal Data in a timely manner in the event of a physical or technical incident, Data importer will ensure that backups of essential information and software, and in particular any Personal Data, are performed on a regular basis and Data importer shall test the backup process regularly.
3. **Physical Security.** Data importer will actively manage the physical security controls and ensure all buildings throughout Data importer's enterprise that house critical IT functions (e.g., data centers, network facilities, and key user areas) and store, process or transmit Personal Data are physically protected from unauthorized access.
4. **Training.** Data importer will provide training on data security and privacy matters so that all members of Data importer who handle Personal Data are trained in these matters.
5. **Information security incident management.** Data importer will maintain policies and procedures to develop a consistent and effective approach to the management of information security incidents.

For transfers to (sub-) processors, also describe the specific technical and organisational measures to be taken by the (sub-) processor to be able to provide assistance to the controller and, for transfers from a processor to a sub-processor, to the data exporter:

Data importer requires its sub-processors to maintain technical and organisational measures at least as protective as those described in this Annex 2.

ANNEX III

LIST OF SUB-PROCESSORS

The importer has authorized the list of sub-processors published on the following web page: https://info.orcid.org/sub-processors

The importer will notify the exporter of any changes to the list of sub-processors, by email 30 days prior to the start of processing by any new sub-processor.

Any objections to the changes should be raised with the importer's contact person named in Annex I.

STANDARDNÍ SMLUVNÍ DOLOŽKY PRO PŘEDÁVÁNÍ OSOBNÍCH ÚDAJŮ DO TŘETÍCH ZEMÍ

SPRÁVCE SPRÁVCI

VZHLEDEM K TOMU, že Národní technická knihovna (dále jen "vedoucí konsorcia"), jednající svým jménem a jako zástupce každého ze členů, které vedoucí konsorcia identifikoval v samoobslužném nástroji ORCID na adrese http://orcid.org/self-service (ve znění, které může vedoucí konsorcia čas od času aktualizovat) (dále společně jen "členové konsorcia"), a společnost ORCID, Inc. (dále jen "ORCID") uzavřely licenční smlouvu pro členy konsorcia;

VZHLEDEM K TOMU, že v souvislosti s touto smlouvou předává vedoucí konsorcia a členové konsorcia určité osobní údaje společnosti ORCID a že společnost ORCID tyto údaje zpracovává;

VZHLEDEM K TOMU, že Evropská komise schválila pro takové předávání a zpracování osobních údajů standardní smluvní doložky v níže uvedené podobě;

VZHLEDEM K TOMU, že vedoucí konsorcia prohlašuje a zaručuje, že má zákonné oprávnění a získal právně přípustné souhlasy k tomu, aby jednal jako zástupce členů konsorcia a zavázal je těmito standardními smluvními doložkami;

VZHLEDEM K TOMU, že vedoucí konsorcia a členové konsorcia jsou pro účely níže uvedeného bodu 1 písm. b) dále společně označováni jako "vývozce údajů";

PROTO NYNÍ se strany za dobrou a cennou protihodnotu, jejíž dostatečnost uznávají, dohodly na tom, že (i) následující standardní smluvní doložky zajišťují vhodné záruky ochrany údajů při mezinárodním předávání a zpracování údajů v souvislosti s licenční smlouvou s členy konsorcia a (ii) že vedoucí konsorcia, členové konsorcia a ORCID jsou těmito standardními smluvními doložkami smluvně vázáni.

ODDÍL I

Doložka 1

Účel a oblast působnosti

(a) Účelem těchto standardních smluvních doložek je zajistit soulad s požadavky nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o ochraně osobních údajů a o volném pohybu těchto údajů (obecné nařízení o ochraně osobních údajů) (1) za účelem předání osobních údajů do třetí země.

(b) Strany:

(i) fyzická nebo právnická osoba (osoby), veřejný orgán (orgány), agentura (agentury) nebo jiný subjekt (subjekty) (dále jen „subjekt (subjekty)") předávající osobní údaje, jak je uvedeno v příloze I.A a v samoobslužném nástroji ORCID na adrese http://orcid.org/self-service (dále jen „vývozce údajů"), a

(ii) subjekt (subjekty) ve třetí zemi, který (které) přijímá (přijímají) osobní údaje od vývozce údajů, přímo nebo nepřímo prostřednictvím jiného subjektu, který je rovněž smluvní stranou těchto doložek a který je uveden v příloze I.A (dále jen „dovozce údajů")

souhlasili s těmito standardními smluvními doložkami (dále jen: „doložky").

(c) Tyto doložky se vztahují na předávání osobních údajů, jak je uvedeno v příloze I.B.

(d) Dodatek k těmto doložkám obsahující přílohy, na které se v nich odkazuje, tvoří nedílnou součást těchto doložek.

Doložka 2

Účinnost a neměnnost doložek

(a) Tyto doložky stanoví vhodné záruky, včetně vymahatelných práv subjektu údajů a účinných opravných prostředků, podle čl. 46 odst. 1 a čl. 46 odst. 2 písm. c) nařízení (EU) 2016/679 a v případě předávání údajů od správců ke zpracovatelům a/nebo od zpracovatelů ke zpracovatelům standardní smluvní doložky podle čl. 28 odst. 7 nařízení (EU) 2016/679, pokud nebudou změněny, s výjimkou výběru příslušného modulu (příslušných modulů) nebo doplnění či aktualizace informací v dodatku. To nebrání smluvním stranám zahrnout standardní smluvní doložky stanovené v

těchto doložkách do širší smlouvy a/nebo přidat další doložky nebo dodatečné záruky, pokud nejsou v přímém či nepřímém rozporu s těmito doložkami nebo se nedotýkají základních práv či svobod subjektů údajů.

(b) Těmito doložkami nejsou dotčeny povinnosti, které se na vývozce údajů vztahují na základě nařízení (EU) 2016/679.

Doložka 3

Oprávněné třetí strany

(a) Subjekty údajů se mohou dovolávat těchto doložek a vymáhat je jako třetí strany vůči vývozci a/nebo dovozci údajů s následujícími výjimkami:

(i) Doložka 1, doložka 2, doložka 3, doložka 6, doložka 7;

(ii) Doložka 8.5 písm. e) a doložka 8.9 písm. b);

(iii) Doložka 12 písm. a) a d);

(iv) Doložka 13;

(v) Doložka 15.1 písm. c), d) a e);

(vi) Doložka 16 písm. e);

(vii) Doložka 18 písm. a) a b).

(b) Odstavcem a) nejsou dotčena práva subjektů údajů podle nařízení (EU) 2016/679.

Doložka 4

Výklad

(a) Pokud se v těchto doložkách používají pojmy definované v nařízení (EU) 2016/679, mají tyto pojmy stejný význam jako v uvedeném nařízení.

(b) Tyto doložky se vykládají ve světle nařízení (EU) 2016/679.

(c) Tyto doložky nelze vykládat v rozporu s právy a povinnostmi stanovenými v nařízení (EU) 2016/679.

Doložka 5

Hierarchie

V případě rozporu mezi těmito doložkami a ustanoveními souvisejících dohod mezi stranami, které existovaly v době sjednání těchto doložek nebo byly uzavřeny později, mají přednost tyto doložky.

Doložka 6

Popis předávání

Podrobnosti o předávání, zejména kategorie předávaných osobních údajů a účel(y) jejich předávání, jsou uvedeny v příloze I.B.

ODDÍL II - POVINNOSTI STRAN

Doložka 8

Záruky ochrany údajů

Vývozce údajů zaručuje, že vynaložil přiměřené úsilí, aby zjistil, zda je dovozce údajů schopen prostřednictvím zavedení vhodných technických a organizačních opatření splnit své povinnosti podle těchto doložek.

8.1 Účelové omezení

Dovozce údajů zpracovává osobní údaje pouze pro konkrétní účel (účely) předání, jak je uvedeno v příloze I.B. Osobní údaje může zpracovávat pouze za jiným účelem:

(i) pokud k tomu získal předchozí souhlas subjektu údajů;

(ii) pokud je to nezbytné pro určení, výkon nebo obhajobu právních nároků v rámci konkrétních správních, regulačních nebo soudních řízení; nebo

(iii) pokud je to nezbytné pro ochranu životně důležitých zájmů subjektu údajů nebo jiné fyzické osoby;

8.2 Transparentnost

(a) Aby subjekty údajů mohly účinně vykonávat svá práva podle doložky10, informuje je dovozce údajů buď přímo, nebo prostřednictvím vývozce údajů:

(i) o jeho identitě a kontaktních údajích;

(ii) o kategoriích zpracovávaných osobních údajů;

(iii) o právu získat kopii těchto doložek;

(iv) v případě, že hodlá osobní údaje dále předat jakékoli třetí straně/stranám, o příjemci nebo o kategorii příjemců (podle potřeby s ohledem na poskytnutí smysluplných informací), účelu takového dalšího předání a důvodu podle doložky 8.7.

(b) Písmeno a) se nepoužije, pokud subjekt údajů již informace má, včetně případů, kdy tyto informace již poskytl vývozce údajů, nebo pokud se poskytnutí informací ukáže jako nemožné nebo by pro dovozce údajů znamenalo nepřiměřené úsilí. V druhém případě dovozce údajů tyto informace v rámci možností zveřejní.

(c) Strany na požádání poskytnou subjektu údajů bezplatně kopii těchto doložek včetně dodatku, který vyplnily. V rozsahu nezbytném pro ochranu obchodního tajemství nebo jiných důvěrných informací, včetně osobních údajů, mohou strany před sdílením kopie upravit část textu dodatku, ale poskytnou smysluplné shrnutí, pokud by jinak subjekt údajů nebyl schopen porozumět jeho obsahu nebo uplatnit svá práva. Strany na požádání poskytnou subjektu údajů důvody pro redigování, pokud je to možné, aniž by došlo k odhalení redigovaných informací.

(d) Odstavci a) až c) nejsou dotčeny povinnosti vývozce údajů podle článků 13 a 14 nařízení (EU) 2016/679.

8.3 Přesnost a minimalizace údajů

(a) Každá strana zajistí, aby osobní údaje byly přesné a v případě potřeby aktualizované. Dovozce údajů přijme veškerá přiměřená opatření, aby zajistil, že osobní údaje, které jsou s ohledem na účel (účely) zpracování nepřesné, budou neprodleně vymazány nebo opraveny.

(b) Pokud jedna ze stran zjistí, že osobní údaje, které předala nebo obdržela, jsou nepřesné nebo zastaralé, informuje o tom bez zbytečného odkladu druhou stranu.

(c) Dovozce údajů zajistí, aby osobní údaje byly přiměřené, relevantní a omezené na to, co je nezbytné vzhledem k účelu (účelům) zpracování.

8.4 Omezení uložení

Dovozce údajů uchovává osobní údaje po dobu ne delší, než je nezbytné pro účely, pro které jsou zpracovávány. Zavede vhodná technická nebo organizační opatření, aby zajistil splnění této povinnosti, včetně výmazu nebo anonymizace (2) údajů a všech záloh na konci doby uchovávání.

8.5 Zabezpečení zpracování

(a) Dovozce údajů a při jejich předávání také vývozce údajů zavede vhodná technická a organizační opatření k zajištění bezpečnosti osobních údajů, včetně ochrany před narušením bezpečnosti vedoucím k náhodnému nebo nezákonnému zničení, ztrátě, změně, neoprávněnému zveřejnění nebo přístupu (dále jen „narušení bezpečnosti osobních údajů"). Při posuzování vhodné úrovně zabezpečení řádně zohlední stav techniky, náklady na provedení, povahu, rozsah, kontext a účel (účely) zpracování a rizika spojená se zpracováním pro subjekt údajů. Strany zejména zváží možnost použití šifrování nebo pseudonymizace, a to i během přenosu, pokud lze tímto způsobem splnit účel zpracování.

(b) Strany se dohodly na technických a organizačních opatřeních uvedených v příloze II. Dovozce údajů provádí pravidelné kontroly, aby zajistil, že tato opatření nadále poskytují odpovídající úroveň bezpečnosti.

(c) Dovozce údajů zajistí, aby se osoby oprávněné zpracovávat osobní údaje zavázaly zachovat mlčenlivost nebo aby se na ně vztahovala odpovídající zákonná povinnost zachovat mlčenlivost.

(d) V případě narušení zabezpečení osobních údajů, které se týká osobních údajů zpracovávaných dovozcem údajů podle těchto doložek, přijme dovozce údajů vhodná opatření k řešení narušení zabezpečení osobních údajů, včetně opatření ke zmírnění jeho možných nepříznivých účinků.

(e) V případě narušení zabezpečení osobních údajů, které by mohlo vést k ohrožení práv a svobod fyzických osob, dovozce údajů bez zbytečného odkladu informuje vývozce údajů i příslušný dozorový úřad podle doložky 13. Toto oznámení musí obsahovat i) popis povahy narušení (pokud možno včetně kategorií a přibližného počtu dotčených subjektů údajů a záznamů osobních údajů), ii) jeho pravděpodobné důsledky, iii) přijatá nebo navrhovaná opatření k řešení narušení a iv) údaje o kontaktním místě, u kterého lze získat další informace. Pokud není možné, aby dovozce údajů poskytl všechny informace najednou, může tak učinit postupně bez zbytečného dalšího prodlení.

(f) V případě narušení zabezpečení osobních údajů, které může mít za následek vysoké riziko pro práva a svobody fyzických osob, dovozce údajů bez zbytečného odkladu oznámí narušení zabezpečení osobních údajů a jeho povahu také dotčeným subjektům údajů, v případě potřeby ve spolupráci s vývozcem údajů, spolu s informacemi uvedenými

v odstavci (e), bodech ii) až iv), ledaže dovozce údajů zavedl opatření k výraznému snížení rizika pro práva nebo svobody fyzických osob nebo by oznámení vyžadovalo nepřiměřené úsilí. V druhém případě dovozce údajů místo toho vydá veřejné sdělení nebo přijme podobné opatření, aby o narušení zabezpečení osobních údajů informoval veřejnost.

(g) Dovozce údajů zdokumentuje všechny relevantní skutečnosti týkající se narušení zabezpečení osobních údajů, včetně jeho důsledků a přijatých nápravných opatření, a vede o tom záznamy.

8.6 Citlivé údaje

Pokud se předávání týká osobních údajů odhalujících rasový nebo etnický původ, politické názory, náboženské nebo filozofické přesvědčení nebo členství v odborech, genetických údajů nebo biometrických údajů za účelem jedinečné identifikace fyzické osoby, údajů týkajících se zdraví nebo sexuálního života nebo sexuální orientace osoby nebo údajů týkajících se odsouzení za trestné činy (dále jen „citlivé údaje"), dovozce údajů uplatní zvláštní omezení a/nebo dodatečná ochranná opatření přizpůsobená zvláštní povaze údajů a souvisejícím rizikům. To může zahrnovat omezení pracovníků, kteří mají k osobním údajům přístup, dodatečná bezpečnostní opatření (např. pseudonymizaci) a/nebo dodatečná omezení týkající se dalšího zpřístupnění.

8.7 Další předávání

Dovozce údajů nepředá osobní údaje třetí straně nacházející se mimo Evropskou unii (3) (ve stejné zemi jako dovozce údajů nebo v jiné třetí zemi, dále jen „další předání"), pokud tato třetí strana není vázána těmito doložkami podle příslušného modulu, nebo s tím nesouhlasí. V opačném případě může dovozce údajů provést další přenos pouze tehdy, pokud:

(a) je to do země, která využívá rozhodnutí o přiměřenosti podle článku 45 nařízení (EU) 2016/679, jež se vztahuje na další předávání;

(b) (ii) třetí strana jinak zajistí vhodné záruky podle článků 46 nebo 47 nařízení (EU) 2016/679 s ohledem na dané zpracování;

(c) třetí strana uzavře s dovozcem údajů závazný nástroj zajišťující stejnou úroveň ochrany údajů jako podle těchto doložek a dovozce údajů poskytne kopii těchto záruk vývozci údajů;

(d) je to nezbytné pro určení, výkon nebo obhajobu právních nároků v rámci konkrétních správních, regulačních nebo soudních řízení;

(e) je to nezbytné pro ochranu životně důležitých zájmů subjektu údajů nebo jiné fyzické osoby; nebo

(f) pokud se neuplatní žádná z ostatních podmínek, dovozce údajů získal výslovný souhlas subjektu údajů s dalším předáním v konkrétní situaci poté, co jej informoval o účelu (účelech), totožnosti příjemce a možných rizicích takového předání pro něj z důvodu neexistence vhodných záruk ochrany údajů. V takovém případě dovozce údajů informuje vývozce údajů a na jeho žádost mu předá kopii informací poskytnutých subjektu údajů.

Jakékoli další předávání údajů je podmíněno tím, že dovozce údajů dodrží všechna ostatní ochranná opatření podle těchto doložek, zejména omezení účelu.

8.8 Zpracování z pověření dovozce údajů

Dovozce údajů zajistí, aby jakákoli osoba jednající z jeho pověření, včetně zpracovatele, zpracovávala údaje pouze na jeho pokyn.

8.9 Dokumentace a plnění povinností

(a) Každá strana musí být schopna prokázat plnění svých povinností podle těchto doložek. Dovozce údajů vede zejména příslušnou dokumentaci o činnostech zpracování prováděných na jeho odpovědnost.

(b) Dovozce údajů tuto dokumentaci na požádání zpřístupní příslušnému dozorovému úřadu.

Doložka 9 *- Záměrně ponecháno prázdné.*

Doložka 10

Práva subjektu údajů

(a) Dovozce údajů, případně s pomocí vývozce údajů, vyřídí veškeré dotazy a žádosti, které obdrží od subjektu údajů a které se týkají zpracování jeho osobních údajů a výkonu jeho práv podle těchto doložek, bez zbytečného odkladu, nejpozději však do jednoho měsíce od obdržení dotazu nebo žádosti. (10) Dovozce údajů přijme vhodná opatření k usnadnění těchto

dotazů, žádosti a výkonu práv subjektu údajů. Veškeré informace poskytované subjektu údajů musí být ve srozumitelné a snadno přístupné formě, za použití jasného a jednoduchého jazyka.

(b) Na žádost subjektu údajů dovozce údajů bezplatně:

(i) poskytne subjektu údajů potvrzení o tom, zda jsou zpracovávány osobní údaje, které se ho týkají, a v takovém případě kopii údajů, které se ho týkají, a informace uvedené v příloze I; pokud byly nebo budou osobní údaje dále předány, poskytne informace o příjemcích nebo kategoriích příjemců (podle potřeby s ohledem na poskytnutí smysluplných informací), kterým byly nebo budou osobní údaje dále předány, účel těchto dalších předání a jejich důvod podle doložky 8.7; a poskytne informace o právu podat stížnost u dozorového úřadu podle doložky 12 písm. c) bodu i);

(ii) opraví nepřesné nebo neúplné údaje týkající se subjektu údajů;

(iii) vymaže osobní údaje týkající se subjektu údajů, pokud tyto údaje jsou nebo byly zpracovávány v rozporu s některým z těchto ustanovení zajišťujících práva třetích stran nebo pokud subjekt údajů odvolá souhlas, na němž je zpracování založeno.

(c) Pokud dovozce údajů zpracovává osobní údaje pro účely přímého marketingu, přestane je pro tyto účely zpracovávat, pokud to subjekt údajů namítne.

(d) Dovozce údajů neprovede rozhodnutí založené výhradně na automatizovaném zpracování předávaných osobních údajů (dále jen „automatizované rozhodnutí"), které by mělo právní účinky pro subjekt údajů nebo se jej podobně významně dotýkalo, ledaže by k tomu dal subjekt údajů výslovný souhlas nebo by k tomu byl oprávněn podle právních předpisů země určení, pokud tyto právní předpisy stanoví vhodná opatření na ochranu práv a oprávněných zájmů subjektu údajů. V takovém případě dovozce údajů dle potřeby ve spolupráci s vývozcem údajů:

(i) informuje subjekt údajů o plánovaném automatizovaném rozhodování, jeho předpokládaných důsledcích a logice a

(ii) zavede vhodné záruky, přinejmenším tím, že umožní subjektu údajů napadnout rozhodnutí, vyjádřit svůj názor a dosáhnout přezkoumání lidskou osobou.

(e) Pokud jsou žádosti od subjektu údajů nepřiměřené, zejména kvůli jejich opakující se povaze, může dovozce údajů buď účtovat přiměřený poplatek zohledňující administrativní náklady na vyhovění žádosti, nebo odmítnout na žádost jednat.

(f) Dovozce údajů může žádost subjektu údajů odmítnout, pokud je takové odmítnutí přípustné podle právních předpisů země určení a je v demokratické společnosti nezbytné a přiměřené k ochraně jednoho z cílů uvedených v čl. 23 odst. 1 nařízení (EU) 2016/679.

(g) Pokud dovozce údajů hodlá žádost subjektu údajů odmítnout, informuje subjekt údajů o důvodech odmítnutí a o možnosti podat stížnost u příslušného dozorového úřadu a/nebo se domáhat soudní ochrany.

Doložka 11

Náprava

(a) Dovozce údajů informuje subjekty údajů transparentním a snadno přístupným způsobem prostřednictvím individuálního oznámení nebo na svých internetových stránkách o kontaktním místě oprávněném vyřizovat stížnosti. Neprodleně vyřizuje všechny stížnosti, které obdrží od subjektu údajů.

(b) V případě sporu mezi subjektem údajů a jednou ze stran ohledně dodržování těchto doložek vynaloží tato strana veškeré úsilí, aby problém včas vyřešila smírnou cestou. Strany se o těchto sporech vzájemně informují a případně spolupracují při jejich řešení.

(c) Pokud subjekt údajů uplatní právo třetí strany jako příjemce podle doložky 3, dovozce údajů přijme rozhodnutí subjektu údajů:

(i) podat stížnost u dozorového úřadu v členském státě svého obvyklého bydliště nebo pracoviště nebo u příslušného dozorového úřadu podle doložky 13;

(ii) postoupit spor příslušnému soudu ve smyslu doložky 18.

(d) Strany souhlasí s tím, že subjekt údajů může být zastoupen neziskovým subjektem, organizací nebo sdružením za podmínek stanovených v čl. 80 odst. 1 nařízení (EU) 2016/679.

(e) Dovozce údajů se řídí rozhodnutím, které je závazné podle platného práva EU nebo členského státu.

(f) Dovozce údajů souhlasí s tím, že volba učiněná subjektem údajů nebude mít vliv na jeho hmotná a procesní práva domáhat se nápravy v souladu s platnými zákony.

Doložka 12

Odpovědnost

(a) Každá strana odpovídá druhé straně/stranám za jakékoli škody, které způsobí druhé straně/stranám porušením těchto doložek.

(b) Každá strana odpovídá subjektu údajů a subjekt údajů má nárok na náhradu jakékoli majetkové nebo nemajetkové újmy, kterou způsobí subjektu údajů porušením práv oprávněné třetí strany podle těchto doložek. Tím není dotčena odpovědnost vývozce údajů podle nařízení (EU) 2016/679.

(c) Pokud je za škodu způsobenou subjektu údajů v důsledku porušení těchto ustanovení odpovědná více než jedna strana, odpovídají všechny odpovědné strany společně a nerozdílně a subjekt údajů je oprávněn podat žalobu u soudu proti kterékoli z těchto stran.

(d) Strany se dohodly, že pokud je jedna strana shledána odpovědnou podle písmene c), je oprávněna požadovat od druhé strany/stran zpět část náhrady škody odpovídající její/jejich odpovědnosti za škodu.

(e) Dovozce údajů se nemůže odvolávat na chování zpracovatele nebo dílčího zpracovatele, aby se vyhnul své vlastní odpovědnosti.

Doložka 13

Dohled

(a) Pokud je vývozce údajů usazen v členském státě EU: Příslušným dozorovým úřadem je dozorový úřad odpovědný za zajištění souladu vývozce údajů s nařízením (EU) 2016/679, pokud jde o předávání údajů, jak je uvedeno v příloze I.C. Pokud vývozce údajů není usazen v členském státě EU, ale spadá do územní působnosti nařízení (EU) 2016/679 v souladu s jeho čl. 3 odst. 2 a jmenoval zástupce podle čl. 27 odst. 1 nařízení (EU) 2016/679: Jako příslušný orgán dozoru působí orgán dozoru členského státu, v němž je usazen zástupce ve smyslu čl. 27 odst. 1 nařízení (EU) 2016/679, jak je uvedeno v příloze I.C.

Pokud vývozce údajů není usazen v členském státě EU, ale spadá do územní působnosti nařízení (EU) 2016/679 v souladu s jeho

článkem 3 (2), aniž by však musel jmenovat zástupce podle čl. 27 odst. 2 nařízení (EU) 2016/679: Příslušným dozorovým úřadem je dozorový úřad jednoho z členských států, v němž se nacházejí subjekty údajů, jejichž osobní údaje jsou předávány podle těchto doložek v souvislosti s nabídkou zboží nebo služeb nebo jejichž chování je sledováno, jak je uvedeno v příloze I.C.

(b) Dovozce údajů souhlasí s tím, že se podřídí pravomoci příslušného dozorového úřadu a bude s ním spolupracovat při všech postupech, jejichž cílem je zajistit dodržování těchto doložek. Dovozce údajů se zejména zavazuje reagovat na dotazy, podrobit se auditům a dodržovat opatření přijatá dozorovým úřadem, včetně nápravných a kompenzačních opatření. Dozorovému orgánu poskytne písemné potvrzení, že byla přijata nezbytná opatření.

ODDÍL III - MÍSTNÍ PRÁVNÍ PŘEDPISY A POVINNOSTI V PŘÍPADĚ PŘÍSTUPU ORGÁNŮ VEŘEJNÉ MOCI

Doložka 14

Místní právní předpisy a postupy mající dopad na dodržování doložek

(a) Strany zaručují, že nemají důvod se domnívat, že právní předpisy a praxe ve třetí zemi určení, které se vztahují na zpracování osobních údajů dovozcem údajů, včetně požadavků na zveřejnění osobních údajů nebo opatření opravňujících k přístupu orgánů veřejné moci, brání dovozci údajů v plnění jeho povinností podle těchto doložek. To vychází z toho, že právní předpisy a postupy, které respektují podstatu základních práv a svobod a nepřekračují rámec toho, co je v demokratické společnosti nezbytné a přiměřené k zajištění jednoho z cílů uvedených v čl. 23 odst. 1 nařízení (EU) 2016/679, nejsou v rozporu s těmito doložkami.

(b) Strany prohlašují, že při poskytování záruky podle písmene a) řádně zohlednily zejména následující prvky:

(i) konkrétní okolnosti předání, včetně délky řetězce zpracování, počtu zúčastněných subjektů a použitých přenosových kanálů; zamýšlená další předání; typ příjemce; účel zpracování; kategorie a formát předávaných osobních údajů; hospodářské odvětví, v němž k předání dochází; místo uložení předávaných údajů;

(ii) právní předpisy a postupy třetí země určení - včetně těch, které vyžadují zpřístupnění údajů orgánům veřejné moci nebo povolují přístup těchto orgánů - relevantní s ohledem na konkrétní okolnosti předání a platná omezení a záruky (12);

(iii) veškerá příslušná smluvní, technická nebo organizační ochranná opatření zavedená jako doplněk k ochranným opatřením podle těchto doložek, včetně opatření uplatňovaných při předávání a zpracování osobních údajů v zemi určení.

(c) Dovozce údajů zaručuje, že při provádění posouzení podle písmene b) vynaložil veškeré úsilí, aby vývozci údajů poskytl příslušné informace, a souhlasí s tím, že bude s vývozcem údajů nadále spolupracovat při zajišťování souladu s těmito doložkami.

(d) Strany se dohodly, že zdokumentují posouzení podle písmene b) a na požádání je poskytnou příslušnému dozorovému úřadu.

(e) Dovozce údajů souhlasí s tím, že vývozce údajů neprodleně uvědomí, pokud má po odsouhlasení těchto doložek a po dobu trvání smlouvy důvod se domnívat, že se na něj vztahují nebo vztahovaly právní předpisy nebo postupy, které nejsou v souladu s požadavky podle písmene a), a to i v důsledku změny právních předpisů třetí země nebo opatření (např. žádosti o zveřejnění), které naznačuje uplatňování těchto předpisů v praxi, jež není v souladu s požadavky uvedenými v písmenu a).

(f) Po oznámení podle písmene e) nebo pokud má vývozce údajů jiný důvod se domnívat, že dovozce údajů již nemůže plnit své povinnosti podle těchto doložek, vývozce údajů neprodleně určí vhodná opatření (např. technická nebo organizační opatření k zajištění bezpečnosti a důvěrnosti), která má vývozce údajů a/nebo dovozce údajů přijmout k řešení situace. Vývozce údajů pozastaví předávání údajů, pokud se domnívá, že nelze zajistit vhodné záruky pro takové předávání, nebo pokud mu to nařídí příslušný dozorový úřad. V takovém případě je vývozce údajů oprávněn vypovědět smlouvu, pokud se týká zpracování osobních údajů podle těchto doložek. Pokud se smlouva týká více než dvou stran, může vývozce údajů uplatnit toto právo na ukončení pouze ve vztahu k příslušné straně, pokud se strany nedohodnou jinak. V případě ukončení smlouvy podle této doložky se použije článek 16 písm. d) a e).

Doložka 15

Povinnosti dovozce údajů v případě přístupu orgánů veřejné moci

15.1 Oznámení

(a) Dovozce údajů se zavazuje, že neprodleně (v případě potřeby s pomocí vývozce údajů) uvědomí vývozce údajů a pokud možno i subjekt údajů, pokud:

(i) obdrží právně závaznou žádost orgánu veřejné moci, včetně soudních orgánů, podle právních předpisů země určení o zpřístupnění osobních údajů předávaných podle těchto doložek; takové oznámení musí obsahovat informace o požadovaných osobních údajích, dožadujícím orgánu, právním základu žádosti a poskytnuté odpovědi; nebo

(ii) se dozví o jakémkoli přímém přístupu orgánů veřejné moci k osobním údajům předávaným podle těchto doložek v souladu s právními předpisy země určení; toto oznámení musí obsahovat veškeré informace, které má dovozce k dispozici.

(b) Pokud je dovozci údajů podle právních předpisů země určení zakázáno informovat vývozce údajů a/nebo subjekt údajů, dovozce údajů souhlasí s tím, že vynaloží veškeré úsilí k získání výjimky z tohoto zákazu, aby co nejdříve sdělil co nejvíce informací. Dovozce údajů souhlasí s tím, že bude dokumentovat své maximální úsilí, aby je mohl na žádost vývozce údajů prokázat.

(c) Je li to podle právních předpisů země určení přípustné, dovozce údajů souhlasí s tím, že bude vývozci údajů po dobu trvání smlouvy v pravidelných intervalech poskytovat co nejvíce relevantních informací o obdržených žádostech (zejména počet žádostí, druh požadovaných údajů, dožadující orgán/orgány, zda byly žádosti napadeny, výsledek těchto napadení atd.).

(d) Dovozce údajů se zavazuje uchovávat informace podle písmen a) až c) po dobu trvání smlouvy a na požádání je zpřístupnit příslušnému dozorovému orgánu.

(e) Odstavci a) až c) není dotčena povinnost dovozce údajů podle doložky 14 písm. e) a doložky 16 neprodleně informovat vývozce údajů, pokud není schopen tyto doložky dodržet.

15.2 Přezkum zákonnosti a minimalizace údajů

(a) Dovozce údajů souhlasí s tím, že přezkoumá zákonnost žádosti o zpřístupnění, zejména zda zůstává v rámci pravomoci udělených dožadujícímu orgánu veřejné moci, a že žádost napadne, pokud po pečlivém posouzení dospěje k závěru, že existují rozumné důvody domnívat se, že je podle právních předpisů země určení, platných závazků podle mezinárodního práva a zásad mezinárodní součinnosti nezákonná. Dovozce údajů musí za stejných podmínek využít možnosti odvolání. Při napadení žádosti dovozce údajů požádá o předběžné opatření s cílem pozastavit účinky žádosti do doby, než příslušný soudní orgán rozhodne o její opodstatněnosti. Požadované osobní údaje nezveřejní, dokud k tomu není vyzván podle platných procesních pravidel. Těmito požadavky nejsou dotčeny povinnosti dovozce údajů podle doložky 14 písm. e).

(b) Dovozce údajů souhlasí s tím, že zdokumentuje své právní posouzení a případné námitky proti žádosti o zpřístupnění údajů a v rozsahu přípustném podle právních předpisů země určení zpřístupní dokumentaci vývozci údajů. Na požádání je rovněž zpřístupní příslušnému dozorovému úřadu.

(c) Dovozce údajů souhlasí s tím, že v odpovědi na žádost o zpřístupnění poskytne minimální přípustné množství informací na základě přiměřeného výkladu žádosti.

ODDÍL IV - ZÁVĚREČNÁ USTANOVENÍ

Doložka 16

Nedodržení doložek a vypovězení

(a) Dovozce údajů neprodleně informuje vývozce údajů, pokud z jakéhokoli důvodu není schopen dodržet tyto doložky.

(b) V případě, že dovozce údajů poruší tyto doložky nebo je nebude schopen splnit, vývozce údajů pozastaví předávání osobních údajů dovozci údajů, dokud nebude znovu zajištěno jejich dodržování nebo nebude ukončena smlouva. Tím není dotčena doložka 14 písm. f).

(c) Vývozce údajů je oprávněn ukončit smlouvu v rozsahu, v jakém se týká zpracování osobních údajů podle těchto doložek, pokud:

(i) vývozce údajů pozastavil předávání osobních údajů dovozci údajů podle písmene b) a dodržování těchto doložek nebylo obnoveno v přiměřené lhůtě a v každém případě do jednoho měsíce od pozastavení;

(ii) dovozce údajů podstatně nebo trvale porušuje tyto doložky; nebo

(iii) dovozce údajů nedodrží závazné rozhodnutí příslušného soudu nebo dozorového úřadu týkající se jeho povinností podle těchto doložek.

V těchto případech informuje příslušný dozorový úřad o tomto nedodržení. Pokud se smlouva týká více než dvou stran, může vývozce údajů uplatnit toto právo na ukončení pouze ve vztahu k příslušné straně, pokud se strany nedohodnou jinak.

(d) Osobní údaje, které byly předány před ukončením smlouvy podle písmene c), budou podle volby vývozce údajů neprodleně vráceny vývozci údajů nebo zcela vymazány. Totéž platí pro jakékoli kopie údajů. Dovozce údajů potvrdí vývozci údajů vymazání údajů. Dokud nejsou údaje vymazány nebo vráceny, dovozce údajů nadále zajišťuje dodržování těchto doložek. V případě, že místní právní předpisy platné pro dovozce údajů zakazují vrácení nebo vymazání předaných osobních údajů, dovozce údajů zaručuje, že bude i nadále zajišťovat dodržování těchto doložek a bude údaje zpracovávat pouze v rozsahu a po dobu, které vyžadují tyto místní právní předpisy.

(e) Každá ze stran může odvolat svůj souhlas s tím, že bude těmito doložkami vázána, pokud (i) Evropská komise přijme rozhodnutí podle čl. 45 odst. 3 nařízení (EU) 2016/679, které se vztahuje na předávání osobních údajů, na něž se tyto doložky vztahují, nebo (ii) se nařízení (EU) 2016/679 stane součástí právního rámce země, do níž jsou osobní údaje předávány. Tím nejsou dotčeny další povinnosti, které se na dané zpracování vztahují podle nařízení (EU) 2016/679.

Doložka 17

Rozhodné právo

Tyto doložky se řídí právem jednoho z členských států EU, pokud toto právo umožňuje práva třetích stran. Strany se dohodly, že se jedná o irské právo.

Doložka 18

Volba soudu a příslušnosti

(a) Veškeré spory vyplývající z těchto doložek budou řešeny soudy členského státu EU.

(b) Strany se dohodly, že jimi budou irské soudy.

(c) Subjekt údajů může rovněž podat žalobu proti vývozci a/nebo dovozci údajů u soudu členského státu, v němž má obvyklé bydliště.

(d) Strany souhlasí s tím, že se podřídí soudní pravomoci těchto soudů.

PŘÍLOHA I

A. SEZNAM STRAN

Vývozce (vývozci) údajů: *[Totožnost a kontaktní údaje vývozce (vývozců) údajů a případně jeho/jejich pověřence pro ochranu osobních údajů a/nebo zástupce v Evropské unii].*

1. Jméno: Národní technická knihovna, příspěvková organizace zřízená Ministerstvem školství, mládeže a tělovýchovy

Adresa: Technická 6/2710, 160 80 Praha 6, Dejvice, Česká republika

Jméno kontaktní osoby, její pozice a kontaktní údaje:

Činnosti související s údaji předávanými podle těchto doložek: Používání ORCID Členských služeb API pro aktualizaci záznamů uložených na Registrační platformě ORCID

Podpis a datum:

……

jménem svým a členů konsorcia.

Role (správce/zpracovatel): Správce

Dovozce (dovozci) údajů: *[Totožnost a kontaktní údaje dovozce údajů, včetně kontaktní osoby odpovědné za ochranu údajů].*

1. Jméno: ORCID, Inc

Adresa: 10411 Motor City Drive, Suite 750, Bethesda MD 20817, Spojené státy americké

Jméno kontaktní osoby, její pozice a kontaktní údaje: Will Simpson; ředitel pro technologie; [redacted]

Činnosti související s údaji předávanými podle těchto doložek: Poskytnutí ORCID

Členské služby API pro aktualizaci záznamů uložených na platformě registru ORCID

Podpis a datum:

Role (správce/zpracovatel): Správce

B. POPIS PŘEDÁVÁNÍ

Kategorie subjektů údajů, jejichž osobní údaje jsou předávány

Předávané osobní údaje se mohou týkat výzkumných pracovníků, zaměstnanců, studentů, žadatelů o grant, recenzentů žadatelů o grant, autorů, editorů, recenzentů časopisů a dalších osob zapojených do činnosti vývozce.

Kategorie předávaných osobních údajů

- jméno (včetně variant jména subjektu údajů), e-mailová adresa, online profily a další profily na sociálních sítích;
- podrobnosti o grantech a finančních prostředcích, které subjekty údajů poskytly nebo o které požádaly;
- podrobnosti o výzkumných pracích a dalších předložených dokumentech (např. recenzovaných publikacích) nebo pracích, které subjekty údajů vypracovaly nebo se na nich podílely;
- údaje o subjektech, s nimiž je subjekt údajů spojen nebo u nichž je zaměstnán;

- údaje o vzdělání, kvalifikaci, oceněních, vyznamenáních, členství, službách a funkcích subjektu údajů (např. hostující vědecký pracovník); a
- veškeré další osobní údaje, které mohou být poskytnuty službě ORCID.

Předávané citlivé údaje (pokud je to relevantní) a uplatňovaná omezení nebo ochranná opatření, která plně zohledňují povahu údajů a související rizika, jako je například přísné omezení účelu, omezení přístupu (včetně přístupu pouze pro zaměstnance, kteří absolvovali specializované školení), vedení záznamů o přístupu k údajům, omezení pro další předávání nebo dodatečná bezpečnostní opatření.

N/A

Četnost přenosu (např. zda se data předávají jednorázově nebo průběžně).

Údaje budou přenášeny průběžně, jak určí vývozce.

Povaha zpracování

Předávané osobní údaje budou předmětem těchto základních procesů zpracování:

- Přijímání dat, včetně shromažďování, přístupu, vyhledávání, zaznamenávání a zadávání dat
- Uchovávání dat, včetně jejich ukládání, organizace a strukturování
- Používání dat, včetně analýzy, konzultací a testování
- Ochrana dat, včetně omezování, šifrování a testování zabezpečení
- Sdílení údajů, včetně jejich zveřejňování, šíření, umožnění přístupu nebo jiného zpřístupnění
- Vrácení dat exportérovi dat nebo subjektu údajů
- Vymazání dat, včetně zničení a vymazání

Účel(y) předávání a dalšího zpracování údajů

Přenos se provádí za účelem aktualizace záznamů vedených na platformě registru ORCID.

Doba, po kterou budou osobní údaje uchovávány, nebo není-li to možné, kritéria použitá pro stanovení této doby

Osobní údaje budou uchovávány tak dlouho, jak to dovozce údajů potřebuje k poskytování služeb, nebo tak dlouho, jak to vyžadují platné právní předpisy.

U předávání (dílčím) zpracovatelům uveďte také předmět, povahu a dobu trvání zpracování

Předmět, povaha a doba trvání zpracování osobních údajů jsou popsány výše.

C. PŘÍSLUŠNÝ DOZOROVÝ ORGÁN

Určení příslušného dozorového orgánu/orgánů v souladu s ustanovením 13

Komise pro ochranu dat, Irsko

PŘÍLOHA II

TECHNICKÁ A ORGANIZAČNÍ OPATŘENÍ, VČETNĚ TECHNICKÝCH A ORGANIZAČNÍCH OPATŘENÍ K ZAJIŠTĚNÍ BEZPEČNOSTI ÚDAJŮ

VYSVĚTLUJÍCÍ POZNÁMKA:

Technická a organizační opatření musí být popsána konkrétně (nikoliv obecně). Viz také obecná připomínka na první straně dodatku, zejména pokud jde o potřebu jasně uvést, která opatření se vztahují na jednotlivé přenosy/soubory převodů.

Popis technických a organizačních opatření zavedených dovozcem (dovozci) údajů (včetně příslušných osvědčení) k zajištění odpovídající úrovně bezpečnosti s ohledem na povahu, rozsah, kontext a účel zpracování a na rizika pro práva a svobody fyzických osob.

1. Bezpečnostní zásady a postupy. Dovozce údajů udržuje program kybernetické bezpečnosti, který dokumentuje zásady, standardy a kontrolní mechanismy, které používá k zabezpečení informací a zdrojů souvisejících se službami. Dokumentace zahrnuje organizační, administrativní, technické a fyzické záruky a standardy odpovídající velikosti a složitosti, rozsahu činností a citlivosti dotčených osobních údajů.

2. Správa sítě.

a. **Protokolování událostí.** Dovozce údajů má a bude zaznamenávat všechny klíčové události související se zabezpečením, včetně činností uživatelů, výjimek, poruch a události souvisejících s bezpečností informací, které budou vytvářeny, uchovávány a pravidelně kontrolovány.

b. **Vzdálený přístup.** Vzdálený přístup k síti obsahující osobní údaje nebo přístup k systémům zákazníka se provádí prostřednictvím zabezpečeného připojení (např. VPN). Veškeré extranetové připojení k systémům zákazníka bude probíhat prostřednictvím zákazníkem schválených a autorizovaných zabezpečených vzdálených připojení.

c. **Kontrola přístupu.** Dovozce údajů zamezí přístup k osobním údajům pouze na oprávněné osoby. Dovozce údajů bude pravidelně kontrolovat přístupová práva uživatelů.

d. **Řízení sítě.** Dovozce údajů zabezpečí všechny datové a komunikační sítě, aby zajistil ochranu osobních údajů.

e. **Kontrola malwaru.** Po celou dobu poskytování jakýchkoli služeb vynaloží dovozce dat přiměřené úsilí, aby zajistil, že služby nebudou obsahovat škodlivý software nebo malware.

f. **Kódování.** Dovozce údajů bude všechny osobní údaje při přenosu a v klidovém stavu šifrovat pomocí standardních šifrovacích řešení.

g. **Hesla a vícefaktorové ověřování.** Pracovníci dovozce údajů budou používat jedinečná hesla, která budou pravidelně aktualizována. Všechna hesla musí zůstat důvěrná a nebudou sdílena mezi zaměstnanci dovozce údajů, dodavateli ani uživateli třetích stran. Dovozce dat zavede vícefaktorové ověřování pro účty s přístupem k osobním údajům a systémům a sítím správce.

h. **Zálohování dat.** Aby byla zajištěna schopnost včas obnovit dostupnost a přístup k osobním údajům v případě fyzického nebo technického incidentu, zajistí dovozce údajů pravidelné zálohování základních informací a softwaru, a zejména všech osobních údajů, a dovozce údajů bude proces zálohování pravidelně testovat.

3. Fyzická bezpečnost Dovozce údajů bude aktivně řídit kontroly fyzické bezpečnosti a zajistí, aby všechny budovy v celém podniku dovozce údajů, v nichž se nacházejí kritické funkce IT (např. datová centra, síťová zařízení a klíčové uživatelské prostory) a v nichž se ukládají, zpracovávají nebo předávají osobní údaje, byly fyzicky chráněny před neoprávněným přístupem.

4. Školení. Dovozce údajů zajistí školení o bezpečnosti údajů a ochraně soukromí tak, aby všichni členové dovozce údajů, kteří nakládají s osobními údaji, byli v těchto záležitostech proškoleni.

5. Řízení incidentů v oblasti bezpečnosti informací. Dovozce údajů bude udržovat zásady a postupy pro vytvoření konzistentního a účinného přístupu k řízení incidentů v oblasti bezpečnosti informací.

STANDARDNÍ SMLUVNÍ DOLOŽKY PRO PŘEDÁVÁNÍ OSOBNÍCH ÚDAJŮ DO TŘETÍCH ZEMÍ

SPRÁVCE ZPRACOVATELI

VZHLEDEM K TOMU, že Národní technická knihovna (dále jen "vedoucí konsorcia"), jednající svým jménem a jako zástupce každého ze členů, které vedoucí konsorcia identifikoval v samoobslužném nástroji ORCID na adrese http://orcid.org/self-service (ve znění, které může vedoucí konsorcia čas od času aktualizovat) (dále společně jen "členové konsorcia"), a společnost ORCID, Inc. (dále jen "ORCID") uzavřely licenční smlouvu pro členy konsorcia;

VZHLEDEM K TOMU, že v souvislosti s touto smlouvou předává vedoucí konsorcia a členové konsorcia určité osobní údaje společnosti ORCID a že společnost ORCID tyto údaje zpracovává;

VZHLEDEM K TOMU, že Evropská komise schválila pro takové předávání a zpracování osobních údajů standardní smluvní doložky v níže uvedené podobě;

VZHLEDEM K TOMU, že vedoucí konsorcia prohlašuje a zaručuje, že má zákonné oprávnění a získal právně přípustné souhlasy k tomu, aby jednal jako zástupce členů konsorcia a zavázal je těmito standardními smluvními doložkami;

VZHLEDEM K TOMU, že vedoucí konsorcia a členové konsorcia jsou pro účely níže uvedeného bodu 1 písm. b) dále společně označováni jako "vývozce údajů";

PROTO NYNÍ se strany za dobrou a cennou protihodnotu, jejíž dostatečnost uznávají, dohodly na tom, že (i) následující standardní smluvní doložky zajišťují vhodné záruky ochrany údajů při mezinárodním předávání a zpracování údajů v souvislosti s licenční smlouvou s členy konsorcia a (ii) že vedoucí konsorcia, členové konsorcia a ORCID jsou těmito standardními smluvními doložkami smluvně vázáni.

ODDÍL I

Doložka 1

Účel a oblast působnosti

(a) Účelem těchto standardních smluvních doložek je zajistit soulad s požadavky nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o ochraně osobních údajů a o volném pohybu těchto údajů (obecné nařízení o ochraně osobních údajů) (1) za účelem předání osobních údajů do třetí země.

(b) Strany:

(i) fyzická nebo právnická osoba (osoby), veřejný orgán (orgány), agentura (agentury) nebo jiný subjekt (subjekty) (dále jen „subjekt/y") předávající osobní údaje, jak je uvedeno v příloze I.A (dále jen „vývozce údajů"), a

(ii) subjekt (subjekty) ve třetí zemi, který (které) přijímá (přijímají) osobní údaje od vývozce údajů, přímo nebo nepřímo prostřednictvím jiného subjektu, který je rovněž smluvní stranou těchto doložek a který je uveden v příloze I.A (dále jen „dovozce údajů")

souhlasili s těmito standardními smluvními doložkami (dále jen: „doložky").

(c) Tyto doložky se vztahují na předávání osobních údajů, jak je uvedeno v příloze I.B.

(d) Dodatek k těmto doložkám obsahující přílohy, na které se v nich odkazuje, tvoří nedílnou součást těchto doložek.

Doložka 2

Účinnost a neměnnost doložek

(a) Tyto doložky stanoví vhodné záruky, včetně vymahatelných práv subjektu údajů a účinných opravných prostředků, podle čl. 46 odst. 1 a čl. 46 odst. 2 písm. c) nařízení (EU) 2016/679 a v případě předávání údajů od správců ke zpracovatelům a/nebo od zpracovatelů ke zpracovatelům standardní smluvní doložky podle čl. 28 odst. 7 nařízení (EU) 2016/679, pokud nebudou změněny, s výjimkou výběru příslušného modulu (příslušných modulů) nebo doplnění či aktualizace informací v dodatku. To nebrání smluvním stranám zahrnout standardní smluvní doložky stanovené v těchto doložkách do širší smlouvy a/nebo přidat další doložky nebo dodatečné záruky, pokud nejsou v přímém či nepřímém rozporu s těmito doložkami nebo se nedotýkají základních práv či svobod subjektů údajů.

(b) Těmito doložkami nejsou dotčeny povinnosti, které se na vývozce údajů vztahují na základě nařízení (EU) 2016/679.

Doložka 3

Oprávněné třetí strany

(a) Subjekty údajů se mohou dovolávat těchto doložek a vymáhat je jako třetí strany vůči vývozci a/nebo dovozci údajů s následujícími výjimkami:
   (i) Doložka 1, doložka 2, doložka 3, doložka 6, doložka 7;
   (ii) Doložka 8.1 písm. b), bod 8.9 písm. a), c), d) a e);
   (iii) Doložka 9 písm. a), c), d) a e);
   (iv) Doložka 12 písm. a), d) a f);
   (v) Doložka 13;
   (vi) Doložka 15.1 písm. c), d) a e);
   (vii) Doložka 16 písm. e);
   (viii) Doložka 18 písm. a) a b).

(b) Odstavcem a) nejsou dotčena práva subjektů údajů podle nařízení (EU) 2016/679.

Doložka 4

Výklad

(a) Pokud se v těchto doložkách používají pojmy definované v nařízení (EU) 2016/679, mají tyto pojmy stejný význam jako v uvedeném nařízení.
(b) Tyto doložky se vykládají ve světle nařízení (EU) 2016/679.
(c) Tyto doložky nelze vykládat v rozporu s právy a povinnostmi stanovenými v nařízení (EU) 2016/679.

Doložka 5

Hierarchie

V případě rozporu mezi těmito doložkami a ustanoveními souvisejících dohod mezi stranami, které existovaly v době sjednání těchto doložek nebo byly uzavřeny později, mají přednost tyto doložky.

Doložka 6

Popis předávání

Podrobnosti o předávání, zejména kategorie předávaných osobních údajů a účel(y) jejich předávání, jsou uvedeny v příloze I.B.

ODDÍL II - POVINNOSTI STRAN

Doložka 8

Záruky ochrany údajů

Vývozce údajů zaručuje, že vynaložil přiměřené úsilí, aby zjistil, zda je dovozce údajů schopen prostřednictvím zavedení vhodných technických a organizačních opatření splnit své povinnosti podle těchto doložek.

8.1 Pokyny

(a) Dovozce údajů zpracovává osobní údaje pouze na základě doložených pokynů vývozce údajů. Vývozce údajů může tyto pokyny vydávat po celou dobu trvání smlouvy.
(b) Dovozce údajů neprodleně informuje vývozce údajů, pokud není schopen tyto pokyny dodržet.

8.2 Účelové omezení

Dovozce údajů zpracovává osobní údaje pouze pro konkrétní účel (účely) předání, jak je uvedeno v příloze I.B, pokud nedostane další pokyny od vývozce údajů.

8.3 Transparentnost

Vývozce údajů poskytne subjektu údajů na jeho žádost bezplatně kopii těchto doložek včetně dodatku vyplněného stranami. V rozsahu nezbytném pro ochranu obchodního tajemství nebo jiných důvěrných informací, včetně opatření popsaných v příloze II a osobních údajů, může vývozce údajů před sdílením kopie upravit část textu dodatku k těmto

doložkám, ale poskytne smysluplné shrnutí, pokud by subjekt údajů jinak nebyl schopen porozumět jeho obsahu nebo uplatnit svá práva. Strany na požádání poskytnou subjektu údajů důvody pro redigování, pokud je to možné, aniž by došlo k odhalení redigovaných informací. Tímto ustanovením nejsou dotčeny povinnosti vývozce údajů podle článků 13 a 14 nařízení (EU) 2016/679.

8.4 Přesnost

Pokud dovozce údajů zjistí, že osobní údaje, které obdržel, jsou nepřesné nebo zastaralé, informuje o tom bez zbytečného odkladu vývozce údajů. V takovém případě spolupracuje dovozce údajů s vývozcem údajů na vymazání nebo opravě údajů.

8.5 Doba zpracování a výmaz nebo vrácení údajů

Dovozce údajů zpracovává údaje pouze po dobu uvedenou v příloze I.B. Po ukončení poskytování služeb zpracování údajů dovozce údajů podle volby vývozce údajů vymaže všechny osobní údaje zpracovávané jménem vývozce údajů a potvrdí vývozci údajů, že tak učinil, nebo vrátí vývozci údajů všechny osobní údaje zpracovávané jeho jménem a vymaže existující kopie. Dokud nejsou údaje vymazány nebo vráceny, dovozce údajů nadále zajišťuje dodržování těchto doložek. V případě, že místní zákony platné pro dovozce údajů zakazují vrácení nebo vymazání osobních údajů, dovozce údajů zaručuje, že bude i nadále zajišťovat dodržování těchto doložek a bude je zpracovávat pouze v rozsahu a po dobu, které vyžadují tyto místní zákony. Tím není dotčena doložka 14, zejména požadavek, aby dovozce údajů podle doložky 14 písm. e) informoval vývozce údajů po celou dobu trvání smlouvy, pokud má důvod se domnívat, že se na něj vztahují nebo vztahovaly právní předpisy nebo postupy, které nejsou v souladu s požadavky podle doložky 14 písm. a).

8.6 Zabezpečení zpracování

(a) Dovozce údajů a při jejich předávání také vývozce údajů zavede vhodná technická a organizační opatření k zajištění bezpečnosti údajů, včetně ochrany před narušením bezpečnosti vedoucím k náhodnému nebo nezákonnému zničení, ztrátě, změně, neoprávněnému zveřejnění nebo přístupu k těmto údajům (dále jen „narušení bezpečnosti osobních údajů"). Při posuzování vhodné úrovně zabezpečení strany řádně zohlední stav techniky, náklady na provedení, povahu, rozsah, kontext a účel (účely) zpracování a rizika spojená se zpracováním pro subjekty údajů. Strany zejména zváží možnost použití šifrování nebo pseudonymizace, a to i během přenosu, pokud lze tímto způsobem splnit účel zpracování. V případě pseudonymizace zůstávají dodatečné informace pro přiřazení osobních údajů konkrétnímu subjektu údajů pokud možno pod výhradní kontrolou vývozce údajů. Při plnění svých povinností podle tohoto odstavce dovozce údajů zavede alespoň technická a organizační opatření uvedená v příloze II. Dovozce údajů provádí pravidelné kontroly, aby zajistil, že tato opatření nadále poskytují odpovídající úroveň bezpečnosti.

(b) Dovozce údajů poskytne přístup k osobním údajům svým zaměstnancům pouze v rozsahu nezbytně nutném pro provádění, správu a monitorování smlouvy. Zajistí, aby se osoby oprávněné zpracovávat osobní údaje zavázaly zachovat mlčenlivost nebo aby se na ně vztahovala odpovídající zákonná povinnost zachovat mlčenlivost;

(c) V případě narušení zabezpečení osobních údajů, které se týká osobních údajů zpracovávaných dovozcem údajů podle těchto doložek, přijme dovozce údajů vhodná opatření k řešení tohoto narušení, včetně opatření ke zmírnění jeho nepříznivých účinků. Dovozce údajů rovněž informuje vývozce údajů bez zbytečného odkladu poté, co se o narušení dozvěděl. Toto oznámení musí obsahovat údaje o kontaktním místě, kde lze získat další informace, popis povahy narušení (pokud možno včetně kategorií a přibližného počtu dotčených subjektů údajů a záznamů osobních údajů), jeho pravděpodobné důsledky a přijatá nebo navrhovaná opatření k řešení narušení, případně včetně opatření ke zmírnění jeho možných nepříznivých účinků. Pokud není možné poskytnout všechny informace najednou, musí počáteční oznámení obsahovat informace, které jsou v té době k dispozici, a další informace musí být poskytnuty bez zbytečného odkladu, jakmile budou k dispozici.

(d) Dovozce údajů spolupracuje s vývozcem údajů a je mu nápomocen, aby vývozce údajů mohl splnit své povinnosti podle nařízení (EU) 2016/679, zejména oznámit tuto skutečnost příslušnému dozorovému úřadu a dotčeným subjektům údajů, a to s ohledem na povahu zpracování a informace, které má dovozce údajů k dispozici.

8.7 Citlivé údaje

Pokud se předávání týká osobních údajů odhalujících rasový nebo etnický původ, politické názory, náboženské nebo filozofické přesvědčení nebo členství v odborech, genetických údajů nebo biometrických údajů za účelem jedinečné identifikace fyzické osoby, údajů týkajících se zdraví nebo sexuálního života nebo sexuální orientace osoby nebo údajů

týkajících se rozsudků v trestních věcech a trestných činů (dále jen „citlivé údaje"), použije dovozce údajů zvláštní omezení a/nebo dodatečná ochranná opatření popsaná v příloze I.B.

8.8 Další předávání

Dovozce údajů sdělí osobní údaje třetí straně pouze na základě doložených pokynů vývozce údajů. Kromě toho mohou být údaje zpřístupněny třetí straně nacházející se mimo Evropskou unii (4) (ve stejné zemi jako dovozce údajů nebo v jiné třetí zemi, dále jen „další předání"), pouze pokud je třetí strana vázána těmito doložkami nebo s tím souhlasí, a to podle příslušného modulu, nebo pokud:

(i) další předání je do země, která využívá rozhodnutí o přiměřenosti podle článku 45 nařízení (EU) 2016/679, které se vztahuje na další předání;
(ii) třetí strana jinak zajistí vhodné záruky podle článku 46 nebo 47 nařízení (EU) 2016/679 s ohledem na dané zpracování;
(iii) další předání je nezbytné pro určení, výkon nebo obhajobu právních nároků v rámci konkrétního správního, regulačního nebo soudního řízení nebo
(iv) další předávání je nezbytné k ochraně životně důležitých zájmů subjektu údajů nebo jiné fyzické osoby.

Jakékoli další předávání údajů je podmíněno tím, že dovozce údajů dodrží všechna ostatní ochranná opatření podle těchto doložek, zejména omezení účelu.

8.9 Dokumentace a plnění povinností

(a) Dovozce údajů neprodleně a odpovídajícím způsobem vyřizuje dotazy vývozce údajů, které se týkají zpracování podle těchto doložek.
(b) Strany musí být schopny prokázat dodržování těchto doložek. Dovozce údajů vede zejména příslušnou dokumentaci o činnostech zpracování prováděných jménem vývozce údajů.
(c) Dovozce údajů zpřístupní vývozci údajů veškeré informace nezbytné k prokázání dodržování povinností stanovených v těchto doložkách a na žádost vývozce údajů umožní v přiměřených intervalech nebo v případě, že se objeví náznaky nedodržování, audity činností zpracování, na něž se vztahují tyto doložky, a přispěje k nim. Při rozhodování o přezkumu nebo auditu může vývozce údajů zohlednit příslušná osvědčení, která má dovozce údajů.
(d) Vývozce údajů se může rozhodnout, zda audit provede sám, nebo zda pověří nezávislého auditora. Audity mohou zahrnovat inspekce v prostorách nebo fyzických zařízeních dovozce údajů a v případě potřeby se provádějí s přiměřeným předstihem.
(e) Strany poskytnou informace uvedené v písmenech b) a c), včetně výsledků případných auditů, na požádání příslušnému orgánu dozoru.

Doložka 9

Využití dílčích zpracovatelů

Dovozce údajů má obecně oprávnění vývozce údajů k zapojení dílčího zpracovatele (dílčích zpracovatelů) z dohodnutého seznamu. Dovozce údajů výslovně písemně informuje vývozce údajů o jakýchkoli zamýšlených změnách v tomto seznamu prostřednictvím přidání nebo nahrazení dílčích zpracovatelů nejméně třicet dní předem, čímž poskytne vývozci údajů dostatečný časový prostor k tomu, aby mohl proti těmto změnám vznést námitky před zapojením dílčího zpracovatele (dílčích zpracovatelů). Dovozce údajů poskytne vývozci údajů informace nezbytné k tomu, aby vývozce údajů mohl uplatnit své právo vznést námitku.

(a) Pokud dovozce údajů najme dílčího zpracovatele k provádění konkrétních činností zpracování (jménem vývozce údajů), učiní tak na základě písemné smlouvy, která stanoví v podstatě stejné povinnosti v oblasti ochrany údajů, jaké jsou podle těchto doložek závazné pro dovozce údajů, a to i pokud jde o práva subjektů údajů jako třetích stran. (8) Strany se dohodly, že dodržením tohoto článku dovozce údajů splní své povinnosti podle článku 8.8. Dovozce údajů zajistí, aby dílčí zpracovatel dodržoval povinnosti, které se na dovozce údajů vztahují podle těchto doložek.
(b) Dovozce údajů poskytne vývozci údajů na jeho žádost kopii takové smlouvy s dílčím zpracovatelem a všech následných změn. V rozsahu nezbytném pro ochranu obchodního tajemství nebo jiných důvěrných informací, včetně osobních údajů, může dovozce údajů text smlouvy před sdílením kopie upravit.

(c) Dovozce údajů zůstává plně odpovědný vývozci údajů za plnění povinností dílčího zpracovatele podle jeho smlouvy s dovozcem údajů. Dovozce údajů oznámí vývozci údajů každé neplnění povinností dílčího zpracovatele podle této smlouvy.

(d) Dovozce údajů sjedná s dílčím zpracovatelem doložku o oprávněné třetí straně, podle níž má vývozce údajů - v případě, že dovozce údajů fakticky zanikl, přestal právně existovat nebo se dostal do platební neschopnosti - právo ukončit smlouvu s dílčím zpracovatelem a dát dílčímu zpracovateli pokyn k vymazání nebo vrácení osobních údajů.

Doložka 10

Práva subjektu údajů

(a) Dovozce údajů neprodleně informuje vývozce údajů o každé žádosti, kterou obdržel od subjektu údajů. Na tuto žádost sám neodpoví, pokud k tomu nebyl oprávněn vývozcem údajů.

(b) Dovozce údajů je nápomocen vývozci údajů při plnění povinnosti reagovat na žádosti subjektů údajů o výkon jejich práv podle nařízení (EU) 2016/679. V tomto ohledu strany v příloze II stanoví vhodná technická a organizační opatření, s přihlédnutím k povaze zpracování, kterým bude pomoc poskytnuta, jakož i rozsah a míru požadované pomoci.

(c) Při plnění povinností podle písmen a) a b) se dovozce údajů řídí pokyny vývozce údajů.

Doložka 11

Náprava

(a) Dovozce údajů informuje subjekty údajů transparentním a snadno přístupným způsobem prostřednictvím individuálního oznámení nebo na svých internetových stránkách o kontaktním místě oprávněném vyřizovat stížnosti. Neprodleně vyřizuje všechny stížnosti, které obdrží od subjektu údajů.

(b) V případě sporu mezi subjektem údajů a jednou ze stran ohledně dodržování těchto doložek vynaloží tato strana veškeré úsilí, aby problém včas vyřešila smírnou cestou. Strany se o těchto sporech vzájemně informují a případně spolupracují při jejich řešení.

(c) Pokud subjekt údajů uplatní právo třetí strany jako příjemce podle doložky 3, dovozce údajů přijme rozhodnutí subjektu údajů:

(i) podat stížnost u dozorového úřadu v členském státě svého obvyklého bydliště nebo pracoviště nebo u příslušného dozorového úřadu podle doložky 13;

(ii) postoupit spor příslušnému soudu ve smyslu doložky 18.

(d) Strany souhlasí s tím, že subjekt údajů může být zastoupen neziskovým subjektem, organizací nebo sdružením za podmínek stanovených v čl. 80 odst. 1 nařízení (EU) 2016/679.

(e) Dovozce údajů se řídí rozhodnutím, které je závazné podle platného práva EU nebo členského státu.

(f) Dovozce údajů souhlasí s tím, že volba učiněná subjektem údajů nebude mít vliv na jeho hmotná a procesní práva domáhat se nápravy v souladu s platnými zákony.

Doložka 12

Odpovědnost

(a) Každá strana odpovídá druhé straně/stranám za jakékoli škody, které způsobí druhé straně/stranám porušením těchto doložek.

(b) Dovozce údajů odpovídá subjektu údajů a subjekt údajů má nárok na náhradu jakékoli majetkové či nemajetkové újmy, kterou dovozce údajů nebo jeho dílčí zpracovatel způsobí subjektu údajů porušením práv oprávněné třetí strany podle těchto doložek.

(c) Bez ohledu na písmeno b) je vývozce údajů odpovědný subjektu údajů a subjekt údajů má nárok na náhradu jakékoli majetkové či nemajetkové újmy, kterou vývozce údajů nebo dovozce údajů (nebo jeho dílčí zpracovatel) způsobí subjektu údajů porušením práv oprávněné třetí strany podle těchto doložek. Tím není dotčena odpovědnost vývozce údajů, a pokud je vývozce údajů zpracovatelem jednajícím jménem správce, ani odpovědnost správce podle nařízení (EU) 2016/679, případně nařízení (EU) 2018/1725.

(d) Strany se dohodly, že pokud je vývozce údajů podle písmene c) odpovědný za škodu způsobenou dovozcem údajů (nebo jeho dílčím zpracovatelem), je oprávněn požadovat od dovozce údajů zpět tu část náhrady škody, která odpovídá odpovědnosti dovozce údajů za škodu.

(e) Pokud je za škodu způsobenou subjektu údajů v důsledku porušení těchto ustanovení odpovědná více než jedna strana, odpovídají všechny odpovědné strany společně a nerozdílně a subjekt údajů je oprávněn podat žalobu u soudu proti kterékoli z těchto stran.

(f) Strany se dohodly, že pokud je jedna strana shledána odpovědnou podle písmene e), je oprávněna požadovat od druhé strany/stran zpět část náhrady škody odpovídající její/jejich odpovědnosti za škodu.

(g) Dovozce údajů se nemůže odvolávat na jednání dílčího zpracovatele, aby se vyhnul své vlastní odpovědnosti.

Doložka 13

Dohled

(a) Pokud je vývozce údajů usazen v členském státě EU: Příslušným dozorovým úřadem je dozorový úřad odpovědný za zajištění souladu vývozce údajů s nařízením (EU) 2016/679, pokud jde o předávání údajů, jak je uvedeno v příloze I.C. Pokud vývozce údajů není usazen v členském státě EU, ale spadá do územní působnosti nařízení (EU) 2016/679 v souladu s jeho čl. 3 odst. 2 a jmenoval zástupce podle čl. 27 odst. 1 nařízení (EU) 2016/679: Jako příslušný orgán dozoru působí orgán dozoru členského státu, v němž je usazen zástupce ve smyslu čl. 27 odst. 1 nařízení (EU) 2016/679, jak je uvedeno v příloze I.C.

Pokud vývozce údajů není usazen v členském státě EU, ale spadá do územní působnosti nařízení (EU) 2016/679 v souladu s jeho čl. 3 odst. 2, aniž by však musel jmenovat zástupce podle čl. 27 odst. 2 nařízení (EU) 2016/679: Příslušným dozorovým úřadem je dozorový úřad jednoho z členských států, v němž se nacházejí subjekty údajů, jejichž osobní údaje jsou předávány podle těchto doložek v souvislosti s nabídkou zboží nebo služeb nebo jejichž chování je sledováno, jak je uvedeno v příloze I.C.

(b) Dovozce údajů souhlasí s tím, že se podřídí pravomoci příslušného dozorového úřadu a bude s ním spolupracovat při všech postupech, jejichž cílem je zajistit dodržování těchto doložek. Dovozce údajů se zejména zavazuje reagovat na dotazy, podrobit se auditům a dodržovat opatření přijatá dozorovým úřadem, včetně nápravných a kompenzačních opatření. Dozorovému orgánu poskytne písemné potvrzení, že byla přijata nezbytná opatření.

ODDÍL III - MÍSTNÍ PRÁVNÍ PŘEDPISY A POVINNOSTI V PŘÍPADĚ PŘÍSTUPU ORGÁNŮ VEŘEJNÉ MOCI

Doložka 14

Místní právní předpisy a postupy mající dopad na dodržování doložek

(a) Strany zaručují, že nemají důvod se domnívat, že právní předpisy a praxe ve třetí zemi určení, které se vztahují na zpracování osobních údajů dovozcem údajů, včetně požadavků na zveřejnění osobních údajů nebo opatření opravňujících k přístupu orgánů veřejné moci, brání dovozci údajů v plnění jeho povinností podle těchto doložek. To vychází z toho, že právní předpisy a postupy, které respektují podstatu základních práv a svobod a nepřekračují rámec toho, co je v demokratické společnosti nezbytné a přiměřené k zajištění jednoho z cílů uvedených v čl. 23 odst. 1 nařízení (EU) 2016/679, nejsou v rozporu s těmito doložkami.

(b) Strany prohlašují, že při poskytování záruky podle písmene a) řádně zohlednily zejména následující prvky:

(i) konkrétní okolnosti předání, včetně délky řetězce zpracování, počtu zúčastněných subjektů a použitých přenosových kanálů; zamýšlená další předání; typ příjemce; účel zpracování; kategorie a formát předávaných osobních údajů; hospodářské odvětví, v němž k předání dochází; místo uložení předávaných údajů;

(ii) právní předpisy a postupy třetí země určení - včetně těch, které vyžadují zpřístupnění údajů orgánům veřejné moci nebo povolují přístup těchto orgánů - relevantní s ohledem na konkrétní okolnosti předání a platná omezení a záruky (12);

(iii) veškerá příslušná smluvní, technická nebo organizační ochranná opatření zavedená jako doplněk k ochranným opatřením podle těchto doložek, včetně opatření uplatňovaných při předávání a zpracování osobních údajů v zemi určení.

(c) Dovozce údajů zaručuje, že při provádění posouzení podle písmene b) vynaložil veškeré úsilí, aby vývozci údajů poskytl příslušné informace, a souhlasí s tím, že bude s vývozcem údajů nadále spolupracovat při zajišťování souladu s těmito doložkami.

(d) Strany se dohodly, že zdokumentují posouzení podle písmene b) a na požádání je poskytnou příslušnému dozorovému úřadu.

(e) Dovozce údajů souhlasí s tím, že vývozce údajů neprodleně uvědomí, pokud má po odsouhlasení těchto doložek a po dobu trvání smlouvy důvod se domnívat, že se na něj vztahují nebo vztahovaly právní předpisy nebo postupy, které nejsou v souladu s požadavky podle písmene a), a to i v důsledku změny právních předpisů třetí země nebo opatření (např. žádosti o zveřejnění), které naznačuje uplatňování těchto předpisů v praxi, jež není v souladu s požadavky uvedenými v písmenu a).

(f) Po oznámení podle písmene e) nebo pokud má vývozce údajů jiný důvod se domnívat, že dovozce údajů již nemůže plnit své povinnosti podle těchto doložek, vývozce údajů neprodleně určí vhodná opatření (např. technická nebo organizační opatření k zajištění bezpečnosti a důvěrnosti), která má vývozce údajů a/nebo dovozce údajů přijmout k řešení situace. Vývozce údajů pozastaví předávání údajů, pokud se domnívá, že nelze zajistit vhodné záruky pro takové předávání, nebo pokud mu to nařídí příslušný dozorový úřad. V takovém případě je vývozce údajů oprávněn vypovědět smlouvu, pokud se týká zpracování osobních údajů podle těchto doložek. Pokud se smlouva týká více než dvou stran, může vývozce údajů uplatnit toto právo na ukončení pouze ve vztahu k příslušné straně, pokud se strany nedohodnou jinak. V případě ukončení smlouvy podle této doložky se použije článek 16 písm. d) a e).

Doložka 15

Povinnosti dovozce údajů v případě přístupu orgánů veřejné moci

15.1 Oznámení

(a) Dovozce údajů se zavazuje, že neprodleně (v případě potřeby s pomocí vývozce údajů) uvědomí vývozce údajů a pokud možno i subjekt údajů, pokud:

(i) obdrží právně závaznou žádost orgánu veřejné moci, včetně soudních orgánů, podle právních předpisů země určení o zpřístupnění osobních údajů předávaných podle těchto doložek; takové oznámení musí obsahovat informace o požadovaných osobních údajích, dožadujícím orgánu, právním základu žádosti a poskytnuté odpovědi; nebo

(ii) se dozví o jakémkoli přímém přístupu orgánů veřejné moci k osobním údajům předávaným podle těchto doložek v souladu s právními předpisy země určení; toto oznámení musí obsahovat veškeré informace, které má dovozce k dispozici.

(b) Pokud je dovozci údajů podle právních předpisů země určení zakázáno informovat vývozce údajů a/nebo subjekt údajů, dovozce údajů souhlasí s tím, že vynaloží veškeré úsilí k získání výjimky z tohoto zákazu, aby co nejdříve sdělil co nejvíce informací. Dovozce údajů souhlasí s tím, že bude dokumentovat své maximální úsilí, aby je mohl na žádost vývozce údajů prokázat.

(c) Je-li to podle právních předpisů země určení přípustné, dovozce údajů souhlasí s tím, že bude vývozci údajů po dobu trvání smlouvy v pravidelných intervalech poskytovat co nejvíce relevantních informací o obdržených žádostech (zejména počet žádostí, druh požadovaných údajů, dožadující orgán/orgány, zda byly žádosti napadeny, výsledek těchto napadení atd.).

(d) Dovozce údajů se zavazuje uchovávat informace podle písmen a) až c) po dobu trvání smlouvy a na požádání je zpřístupnit příslušnému dozorovému orgánu.

(e) Odstavci a) až c) není dotčena povinnost dovozce údajů podle doložky 14 písm. e) a doložky 16 neprodleně informovat vývozce údajů, pokud není schopen tyto doložky dodržet.

15.2 Přezkum zákonnosti a minimalizace údajů

(a) Dovozce údajů souhlasí s tím, že přezkoumá zákonnost žádosti o zpřístupnění, zejména zda zůstává v rámci pravomocí udělených dožadujícímu orgánu veřejné moci, a že žádost napadne, pokud po pečlivém posouzení dospěje k závěru, že existují rozumné důvody domnívat se, že je podle právních předpisů země určení, platných závazků podle mezinárodního práva a zásad mezinárodní součinnosti nezákonná. Dovozce údajů musí za stejných podmínek využít možnosti odvolání. Při napadení žádosti dovozce údajů požádá o předběžné opatření s cílem pozastavit účinky žádosti do doby, než příslušný soudní orgán rozhodne o její opodstatněnosti. Požadované osobní údaje nezveřejní, dokud k tomu není vyzván podle platných procesních pravidel. Těmito požadavky nejsou dotčeny povinnosti dovozce údajů podle doložky 14 písm. e).

(b) Dovozce údajů souhlasí s tím, že zdokumentuje své právní posouzení a případné námitky proti žádosti o zpřístupnění údajů a v rozsahu přípustném podle právních předpisů země určení zpřístupní dokumentaci vývozci údajů. Na požádání je rovněž zpřístupní příslušnému dozorovému úřadu.

(c) Dovozce údajů souhlasí s tím, že v odpovědi na žádost o zpřístupnění poskytne minimální přípustné množství informací na základě přiměřeného výkladu žádosti.

ODDÍL IV - ZÁVĚREČNÁ USTANOVENÍ

Doložka 16

Nedodržení doložek a vypovězení

(a) Dovozce údajů neprodleně informuje vývozce údajů, pokud z jakéhokoli důvodu není schopen tyto doložky dodržet.

(b) V případě, že dovozce údajů poruší tyto doložky nebo je nebude schopen splnit, vývozce údajů pozastaví předávání osobních údajů dovozci údajů, dokud nebude znovu zajištěno jejich dodržování nebo nebude ukončena smlouva. Tím není dotčena doložka 14 písm. f).

(c) Vývozce údajů je oprávněn ukončit smlouvu v rozsahu, v jakém se týká zpracování osobních údajů podle těchto doložek, pokud:

(i) vývozce údajů pozastavil předávání osobních údajů dovozci údajů podle písmene b) a dodržování těchto doložek nebylo obnoveno v přiměřené lhůtě a v každém případě do jednoho měsíce od pozastavení;

(ii) dovozce údajů podstatně nebo trvale porušuje tyto doložky; nebo

(iii) dovozce údajů nedodrží závazné rozhodnutí příslušného soudu nebo dozorového úřadu týkající se jeho povinností podle těchto doložek.

V těchto případech informuje příslušný dozorový úřad o tomto nedodržení. Pokud se smlouva týká více než dvou stran, může vývozce údajů uplatnit toto právo na ukončení pouze ve vztahu k příslušné straně, pokud se strany nedohodnou jinak.

(d) Osobní údaje, které byly předány před ukončením smlouvy podle písmene c), budou podle volby vývozce údajů neprodleně vráceny vývozci údajů nebo zcela vymazány. Totéž platí pro jakékoli kopie údajů. Dovozce údajů potvrdí vývozci údajů vymazání údajů. Dokud nejsou údaje vymazány nebo vráceny, dovozce údajů nadále zajišťuje dodržování těchto doložek. V případě, že místní právní předpisy platné pro dovozce údajů zakazují vrácení nebo vymazání předaných osobních údajů, dovozce údajů zaručuje, že bude i nadále zajišťovat dodržování těchto doložek a bude údaje zpracovávat pouze v rozsahu a po dobu, které vyžadují tyto místní právní předpisy.

(e) Každá ze stran může odvolat svůj souhlas s tím, že bude těmito doložkami vázána, pokud (i) Evropská komise přijme rozhodnutí podle čl. 45 odst. 3 nařízení (EU) 2016/679, které se vztahuje na předávání osobních údajů, na něž se tyto doložky vztahují, nebo (ii) se nařízení (EU) 2016/679 stane součástí právního rámce země, do níž jsou osobní údaje předávány. Tím nejsou dotčeny další povinnosti, které se na dané zpracování vztahují podle nařízení (EU) 2016/679.

Doložka 17

Rozhodné právo

Doložky se řídí právem členského státu EU, ve kterém sídlí vývozce údajů. Pokud takové právo neumožňuje práva třetích stran, řídí se právem jiného členského státu EU, které práva třetích stran umožňuje. Strany se dohodly, že se jedná o irské právo.

Doložka 18

Volba soudu a příslušnosti

(a) Veškeré spory vyplývající z těchto doložek budou řešeny soudy členského státu EU.

(b) Strany se dohodly, že jimi budou irské soudy.

(c) Subjekt údajů může rovněž podat žalobu proti vývozci a/nebo dovozci údajů u soudu členského státu, v němž má obvyklé bydliště.

(d) Strany souhlasí s tím, že se podřídí soudní pravomoci těchto soudů.

PŘÍLOHA I

A. SEZNAM STRAN

Vývozce (vývozci) údajů: *[Totožnost a kontaktní údaje vývozce (vývozců) údajů a případně jeho/jejich pověřence pro ochranu osobních údajů a/nebo zástupce v Evropské unii].*

1. Jméno: Národní technická knihovna, příspěvková organizace zřízená Ministerstvem školství, mládeže a tělovýchovy

Adresa: Technická 6/2710, 160 80 Praha 6, Dejvice, Česká republika

Jméno kontaktní osoby, její pozice a kontaktní údaje:

Činnosti související s údaji předávanými podle těchto doložek: Využití poskytované služby umožňující správu členství vývozce v ORCID a nástrojů pro aktualizaci záznamů vedených na platformě registru ORCID.

Podpis a datum:

Role (správce/zpracovatel): Správce

Dovozce (dovozci) údajů: *[Totožnost a kontaktní údaje dovozce údajů, včetně kontaktní osoby odpovědné za ochranu údajů].*

1. Jméno: ORCID, Inc

Adresa: 10411 Motor City Drive, Suite 750, Bethesda MD 20817, Spojené státy americké

Jméno kontaktní osoby, její pozice a kontaktní údaje: Will Simpson; ředitel pro technologie; [redacted]

Činnosti související s údaji předávanými podle těchto doložek: Poskytování služby dovozci, která umožňuje správu jeho členství v ORCID, a nástrojů pro aktualizaci záznamů na platformě registru ORCID

Podpis a datum:

Role (správce/zpracovatel): Zpracovatel

B. POPIS PŘEDÁVÁNÍ

Kategorie subjektů údajů, jejichž osobní údaje jsou předávány

Předávané osobní údaje se mohou týkat výzkumných pracovníků, zaměstnanců, studentů, žadatelů o grant, recenzentů žadatelů o grant, autorů, editorů, recenzentů časopisů a dalších osob zapojených do činnosti vývozce.

Kategorie předávaných osobních údajů

- jméno (včetně variant jména subjektu údajů), e-mailová adresa, online profily a další profily na sociálních sítích
- podrobnosti o grantech a finančních prostředcích, které subjekty údajů poskytly nebo o které požádaly
- podrobnosti o vědeckých pracích a dalších předložených dokumentech (např. recenzovaných publikacích) nebo pracích, které subjekty údajů vypracovaly nebo se na nich podílely
- údaje o subjektech, s nimiž je subjekt údajů spojen nebo u nichž je zaměstnán
- údaje o vzdělání, kvalifikaci, oceněních, vyznamenáních, členství, službách a funkcích subjektu údajů (např. hostující vědecký pracovník)
- veškeré další osobní údaje, které mohou být poskytnuty ORCID

Předávané citlivé údaje (pokud je to relevantní) a uplatňovaná omezení nebo ochranná opatření, která plně zohledňují povahu údajů a související rizika, jako je například přísné omezení účelu, omezení přístupu (včetně přístupu pouze pro zaměstnance, kteří absolvovali specializované školení), vedení záznamů o přístupu k údajům, omezení pro další předávání nebo dodatečná bezpečnostní opatření.

N/A

Četnost přenosu (např. zda se data předávají jednorázově nebo průběžně).

Údaje budou přenášeny průběžně, jak určí vývozce.

Povaha zpracování

Předávané osobní údaje budou předmětem těchto základních procesů zpracování:

- Přijímání dat, včetně shromažďování, přístupu, vyhledávání, zaznamenávání a zadávání dat
- Uchovávání dat, včetně jejich ukládání, organizace a strukturování
- Používání dat, včetně analýzy, konzultací a testování
- Ochrana dat, včetně omezování, šifrování a testování zabezpečení
- Sdílení údajů, včetně jejich zveřejňování, šíření, umožnění přístupu nebo jiného zpřístupnění
- Vrácení údajů vývozci údajů nebo subjektu údajů
- Vymazání dat, včetně zničení a vymazání

Účel(y) předávání a dalšího zpracování údajů

Poskytování služby dovozci, která umožňuje správu jeho členství v ORCID, a nástrojů pro aktualizaci záznamů uložených na platformě registru ORCID.

Doba, po kterou budou osobní údaje uchovávány, nebo není-li to možné, kritéria použitá pro stanovení této doby.

Osobní údaje budou uchovávány tak dlouho, jak to dovozce údajů potřebuje k poskytování služeb, nebo tak dlouho, jak to vyžadují platné právní předpisy.

U předávání (dílčím) zpracovatelům uveďte také předmět, povahu a dobu trvání zpracování

Předmět, povaha a doba trvání zpracování osobních údajů jsou popsány výše."

C. PŘÍSLUŠNÝ DOZOROVÝ ORGÁN

Určení příslušného dozorového orgánu/orgánů v souladu s ustanovením 13

Komise pro ochranu dat, Irsko

PŘÍLOHA II

TECHNICKÁ A ORGANIZAČNÍ OPATŘENÍ, VČETNĚ TECHNICKÝCH A ORGANIZAČNÍCH OPATŘENÍ K ZAJIŠTĚNÍ BEZPEČNOSTI ÚDAJŮ

Popis technických a organizačních opatření zavedených dovozcem (dovozci) údajů (včetně příslušných osvědčení) k zajištění odpovídající úrovně bezpečnosti s ohledem na povahu, rozsah, kontext a účel zpracování a na rizika pro práva a svobody fyzických osob.

1. Bezpečnostní zásady a postupy. Dovozce údajů udržuje program kybernetické bezpečnosti, který dokumentuje zásady, standardy a kontrolní mechanismy, které používá k zabezpečení informací a zdrojů souvisejících se službami. Dokumentace zahrnuje organizační, administrativní, technické a fyzické záruky a standardy odpovídající velikosti a složitosti, rozsahu činnosti a citlivosti dotčených osobních údajů.

2. Správa sítě.

a. Protokolování událostí. Dovozce údajů má a bude zaznamenávat všechny klíčové události související se zabezpečením, včetně činností uživatelů, výjimek, poruch a událostí souvisejících s bezpečností informací, které budou vytvářeny, uchovávány a pravidelně kontrolovány.

b. Vzdálený přístup. Vzdálený přístup k síti obsahující osobní údaje nebo přístup k systémům zákazníka se provádí prostřednictvím zabezpečeného připojení (např. VPN). Veškeré extranetové připojení k systémům zákazníka bude probíhat prostřednictvím zákazníkem schválených a autorizovaných zabezpečených vzdálených připojení.

c. **Kontrola přístupu.** Dovozce údajů zamezí přístup k osobním údajům pouze na oprávněné osoby. Dovozce údajů bude pravidelně kontrolovat přístupová práva uživatelů.

d. Řízení sítě. Dovozce údajů zabezpečí všechny datové a komunikační sítě, aby zajistil ochranu osobních údajů.

e. Kontrola malwaru. Po celou dobu poskytování jakýchkoli služeb vynaloží dovozce dat přiměřené úsilí, aby zajistil, že služby nebudou obsahovat škodlivý software nebo malware.

f. **Kódování.** Dovozce údajů bude všechny osobní údaje při přenosu a v klidovém stavu šifrovat pomocí standardních šifrovacích řešení.

g. Hesla a vícefaktorové ověřování. Pracovníci dovozce údajů budou používat jedinečná hesla, která budou pravidelně aktualizována. Všechna hesla musí zůstat důvěrná a nebudou sdílena mezi zaměstnanci dovozce údajů, dodavateli ani uživateli třetích stran. Dovozce dat zavede vícefaktorové ověřování pro účty s přístupem k osobním údajům a systémům a sítím správce.

h. Zálohování dat. Aby byla zajištěna schopnost včas obnovit dostupnost a přístup k osobním údajům v případě fyzického nebo technického incidentu, zajistí dovozce údajů pravidelné zálohování základních informací a softwaru, a zejména všech osobních údajů, a dovozce údajů bude proces zálohování pravidelně testovat.

3. Fyzická bezpečnost. Dovozce údajů bude aktivně řídit kontroly fyzické bezpečnosti a zajistí, aby všechny budovy v celém podniku dovozce údajů, v nichž se nacházejí kritické funkce IT (např. datová centra, síťová zařízení a klíčové uživatelské prostory) a v nichž se ukládají, zpracovávají nebo předávají osobní údaje, byly fyzicky chráněny před neoprávněným přístupem.

4. Školení. Dovozce údajů zajistí školení o bezpečnosti údajů a ochraně soukromí tak, aby všichni členové dovozce údajů, kteří nakládají s osobními údaji, byli v těchto záležitostech proškoleni.

5. Řízení incidentů v oblasti bezpečnosti informací. Dovozce údajů bude udržovat zásady a postupy pro vytvoření konzistentního a účinného přístupu k řízení incidentů v oblasti bezpečnosti informací.

V případě předávání údajů (dílčím) zpracovatelům rovněž popište konkrétní technická a organizační opatření, která má (dílčí) zpracovatel přijmout, aby byl schopen poskytnout pomoc správci a v případě předávání údajů od zpracovatele dílčímu zpracovateli také vývozci údajů:

Dovozce údajů požaduje, aby jeho dílčí zpracovatelé dodržovali technická a organizační opatření, která jsou přinejmenším stejně ochranná jako opatření popsaná v této příloze 2.

PŘÍLOHA III

SEZNAM DÍLČÍCH ZPRACOVATELŮ

Dovozce autorizoval seznam dílčích zpracovatelů zveřejněný na této webové stránce:

https: //info.orcid.org/sub-processors

Dovozce oznámí vývozci veškeré změny v seznamu dílčích zpracovatelů e-mailem 30 dni před zahájením zpracování jakýmkoli novým dílčím zpracovatelem.

Případné námitky proti změnám je třeba vznést u kontaktní osoby dovozce uvedené v příloze I.