ZMĚNOVÝ POŽADAVEK ZP011_GFŘ

NÁVRH NA ZMĚNU SLUŽBY (ZP)

ID	Projekt GFŘ
Objednatel	GFŘ
Krátký název ZP	**Weby GFŘ/Azure – aktualizace**
Datum podání	7.6. 2022
Datum aktualizace ZP	
Priorita	Střední
Předkladatel	GFŘ, [redacted], vedoucí Projektu za Objednatele
Zhotovitel	SPCSS, [redacted], manažer služby za Poskytovatele

1. Zadání

1.1 Shrnutí zadání

Předmětem zadání změnového požadavku je aktualizace Katalogového listu GFŘ/005 Hosting. Poskytovatel služby zajistí infrastrukturu a servery SPCSS pro provoz portálů www.etrzby.cz a epodpora.mfcr.cz.

Poskytování služby bude zajištěno pomocí cloudových služeb SPCSS. Nedochází ke změně technického správce dotčených domén, ani jejich vlastnictví.

1.2 Zadání požadované změny

1.2.1 Popis požadované změny

Využití cloudové infrastruktury a serverů SPCSS pro provoz portálů

- www.etrzby.cz;
- epodpora.mfcr.cz.

1.2.2 Dopady na stávající Službu

Proběhne aktualizace Katalogového listu GFŘ/005.

1.2.3 Specifikace SW a HW požadavků

Není relevantní

1.3 Popis zajištění realizace změny

Změny zajistí SPCSS v součinnosti s GFŘ.

1.4 Zdůvodnění změny

Záměrem je provést revizi stávající služby, dle Katalogového listu GFŘ/005 – Hosting (pro informační a webové portály GFŘ) z důvodu upřesnění činností, která jsou součástí poskytované služby.

1.5 Očekávané důsledky

Aktualizovat Katalogový list GFŘ/005, včetně detailu popisu služby a aktualizace technické dokumentace.

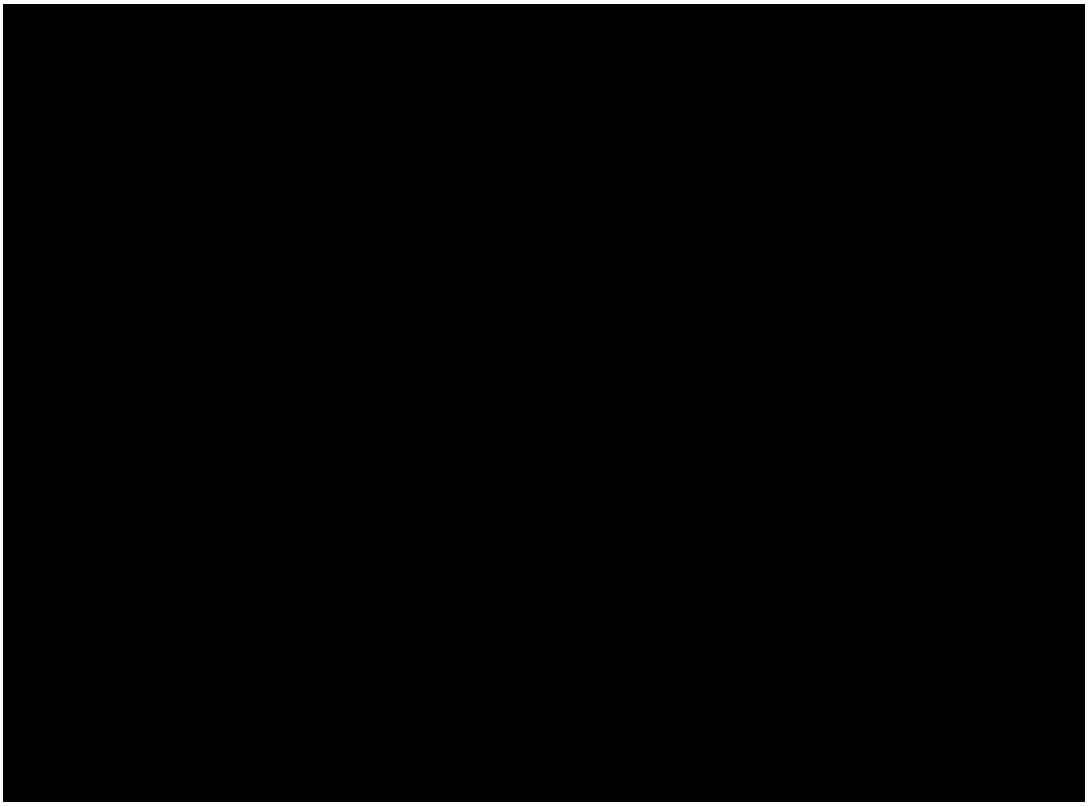
VÝSLEDEK	☒ Dále zpracovávat ☐ Nerealizovat ☐ Přepracovat ☐ Odložit

	Schválil (SPCSS)	**Schválil (GFŘ)**
Jméno	[redacted] manažer služby za SPCSS	[redacted] vedoucí Projektu za GFŘ
Datum dle elektronického podpisu)	31.3.2023	04.04.2023
Podpis		

2. Analýza ZP – technické řešení

2.1 Detailní popis řešení

2.1.1 Popis současného stavu



Systém je provozován na 4 IIS serverech a jednom SQL serveru, umístěných za dvojicí loadbalancerů Citrix NetScaler, které rozvažují zátěž mezi jednotlivé webové servery na kterých jsou provozovány webové portály. Skrz privátní síť Govbone a pak následně pomocí s-2-s VPN tunelu dochází v pravidelných intervalech k updatování obsahu jednotlivých portálových řešení.

Site-2-site tunel je zřízen z infrastruktury SPCSS, kdy na firewaalu SPCSS je zakončeno připojení privátní sítě Govbone a veškerý provoz z IP rozsahu GFŘ z tohoto přiípojení je směrován na VPN koncentrátor Cisco Firepower a dále pak přes již zmiňovaný VPN tunel do prostředí MS Azure, konkrétně do subskripce Z908-15 GFR-WEB. Za update obsahu webových portálů zodpovídá zákazník, potažmo jeho dodavatel.

V cloudovém prostředí MS Azure je kromě produkčního prostředí provozováno ještě prostředí testovací. Obě prostředí jsou pod provozním monitoringem Azure Insights a pod bezpečnostním monitoringem Azure Sentinel. Pro správu a přístup administrátorů zákazníka je zřízen a provozován v prostředí MS Azure tzv. „jump" server, přes který je možné, až dvěma administrátorům současně, přistoupit pomocí RDP protokolu ke správě a nastavení portálových, webových a také databázového serveru.

2.1.2 Cílový stav

V cílovém stavu dochází k několika změnám ve složení jednotlivých prostředí. V první řadě dochází k ukončení testovacího prostředí, které již není potřebné a odstranění některých nepotřebných zdrojů v produkčním prostředí (jednalo se zejména o nevyužívané veřejné IP adresy, nevyužívaný loadbalancer, virtuální servery a síťové interface. Níže uvedené architektonické schéma zobrazuje a odráží aktuální stav celého projektu.

2.2 Předmět služby

Předmětem aktualizované Služby je zajištění infrastruktury a serverů SPCSS pro provoz portálů www.etrzby.cz a epodpora.mfcr.cz. Pro původně provozovaný portál www.daneelektronicky.cz je zajištěno přesměrování do infrastruktury GFŘ, která zajišťuje jeho provoz.

Poskytování služby bude zajištěno pomocí cloudových služeb SPCSS. Nedochází ke změně technického správce dotčených domén, ani jejich vlastnictví. Správu aplikace a obsahu zajišťuje Objednatel.

Pro službu je použitá služba Azure Backup s pravidelným zálohováním všech instalovaných virtuálních serverů, 1x denně s retencí 4 týdnů. Zároveň je řešení zapojeno do systému monitoringu OMS (Application Insight).

2.3 Popis Služby

Součástí Služby je:

- Správa OS;
- Správa DB;
- Správa IIS;
- Loadbalancing.

Pro službu je použitá služba Azure Backup s pravidelným zálohováním všech instalovaných virtuálních serverů, 1x denně s retencí 4 týdnů. Zároveň je řešení zapojeno do systému monitoringu OMS (Application Insight).

2.3.1 Správa OS

Služba obsahuje správu operačních systémů na úrovni virtuálních serverů. Administrátorské účty OS jsou v rukou Poskytovatele. Objednatel používá pro implementaci a podporu provozu aplikací uživatelské účty, využití administrátorských účtů je možné pouze se součinností Poskytovatele nebo bezpečným mechanismem schváleným Poskytovatelem. Součástí služby pro OS MS Windows je i zajištění externí podpory formou MS Premier support.

Správa OS – jednotlivé činnosti

Správa OS zahrnuje následující činnosti:

- Administrace operačních systémů;
- Aktualizace operačních systémů (instalace patchů a security patchů) na základě doporučení výrobce, požadavků Objednatele a s ohledem na stabilitu provozu aplikací;
- Kontrola existence bezpečnostních patchů OS a analýza jejich dopadů na provoz;
- Provádění restartů operačních systémů dle požadavků Objednatele;
- Změny konfigurací OS;
- Vyhodnocování výstupů z monitoringu a reportování výkonů a zatížení (expertní konzultační práce nad výstupy, které jsou součástí běžného provozu);
- Profylaxe systému dle harmonogramu v měsíčních intervalech;
- Součinnosti s případnou instalací a konfigurací nového software;
- Instalace a údržba ovladačů a firmware hardwaru;
- Instalace a údržba certifikátů doporučených Poskytovatelem aplikace pro zabezpečení přístupů na servery;
- Správa lokálních uživatelských účtů v OS;
- Úpravy výkonnostních parametrů systému;
- Správa souborového systému (filesystem, přístupová práva a naplněnost);
- Testování změn provedených v OS;

- Komunikace a řešení problémů s externí L3 podporou;
- Konfigurace a provozování antiviru.

2.3.2 Správa DB

Služba obsahuje správu databázového serveru. Administrátorské účty jsou v rukou Poskytovatele. Objednatel používá pro implementaci a podporu provozu aplikací uživatelské účty, využití administrátorských účtů je možné pouze se součinností Poskytovatele nebo bezpečným mechanismem schváleným Poskytovatelem.

Služba správy databází je poskytována nad Microsoft SQL, aktuálně ve verzi MS SQL 2016 Standard.

Správa DB – jednotlivé činnosti

Správa OS zahrnuje následující činnosti:

- Administrace databáze (změny konfigurací databáze, správa účtů v databázi);
- Instalace patchů a kritických oprav na vyžádání Objednatele;
- Upgrade a migrace databáze na vyžádání Objednatele;
- Definice zálohování a obnovy dat;
- Vyhodnocování výstupů z monitoringu databáze (sledování výkonnostních parametrů a zatížení databáze);
- Úpravy výkonnostních parametrů databáze;
- Reportování výstupů z monitoringu na vyžádání;
- Preventivní údržba databázového serveru;
- Restarty databází dle požadavků Objednatele;
- Odpovídání na technické dotazy při poskytování podpory uživatelům;
- Údržba dokumentace o konfiguraci databáze;
- Testování změn provedených v databázi;
- Komunikace a řešení problémů s externí L3 podporou;

2.3.3 Správa IIS

Služba obsahuje správu IIS na úrovni virtuálních serverů. Administrátorské účty OS jsou v rukou Poskytovatele. Objednatel používá pro implementaci a podporu provozu aplikací uživatelské účty, využití administrátorských účtů je možné pouze se součinností Poskytovatele nebo bezpečným mechanismem schváleným Poskytovatelem.

Správa IIS – jednotlivé činnosti

Správa IIS zahrnuje následující činnosti:

- Instalace IIS;
- Vytváření webových site, virtuálních adresářů;
- Provádění restartů site dle požadavků Objednatele;

- Změny konfigurací IIS;
- Komunikace a řešení problémů s externí L3 podporou;
- Instalace patchů a kritických oprav na vyžádání Objednatele;
- Upgrade a migrace IIS na vyžádání Objednatele;
- Vyhodnocování výstupů z monitoringu;
- Úpravy výkonnostních parametrů;
- Reportování výstupů z monitoringu na vyžádání;
- Preventivní údržba IIS;
- Restarty IIS dle požadavků Objednatele;
- Odpovídání na technické dotazy při poskytování podpory uživatelům.

2.3.4 Loadbalancing

Služba loadbalancing poskytuje funkce inteligentního směrování příchozího provozu dle předem stanovených podmínek tzv. Loadbalancing a terminaci SSL provozu (SSL offloading). Služba je dostupná v obou datových centrech. Rozkládání zátěže lze realizovat různými způsoby. Nejčastěji se používá rovnoměrné rozkládání zátěže mezi všechny cílové servery nebo rozkládání zátěže dle aktuálního vytížení cílových serverů. Další možností je zajištění vysoké dostupnosti cílových serverů mezi datovými centry. Příchozí komunikaci lze nastavit tak, aby byla zpracována servery jednoho datového centra, obou datových center nebo bylo možné provádět řízené odstavení serverů jednoho nebo druhého datového centra. Pokud dojde k výpadku serverů, klient tento výpadek nezaznamená. Služba je poskytována bez přerušení provozu dále.

Loadbalancing - jednotlivé činnosti

Služba loadbalancing zahrnuje následující činnosti:

- Analýza požadavků Objednatele - není součást paušálního plnění;
- Zpracování návrhu architektury řešení - není součást paušálního plnění;
- Provozní správa konfigurací;
- Zpracování provozních požadavků -vypnutí zapnutí loadbalanceru, přidání/ odebrání serverů ze serverové farmy loadbalanceru;
- Aktualizace SW,
- Správa certifikátů – zrušení expirovaných a nahrání platných certifikátů

Předpokladem správné funkce SSL offloading, na těchto zařízeních, je správný SSL certifikát, který je nastaven přesně na míru publikované aplikační OU (organisation unit etrzby.cz, epodpora.mfcr.cz) a jehož délka bude odpovídat minimálně 2K. Certifikát pro webové aplikace (etrzby.cz, epodpora.mfcr.cz) dodává a vlastní Objednatel (GFŘ) minimálně čtrnáct dní před vypršením platnosti starého certifikátu jehož platnost i hlídá.

SPCSS je zodpovědný za výměnu certifikátů. Certifikát bude předán bezpečným způsobem.

2.3.5 Nahrání nového obsahu

Poskytovatel neodpovídá za nahrávání nového obsahu webů. Nahrávání obsahu webových stránek je v zodpovědnosti Objednatele. Poskytovatel poskytne nezbytnou součinnost pro nahrávání obsahu webových stránek.

2.3.6 Monitoring pro GFŘ

Objednateli budou zpřístupněna data monitorovacích nástrojů SPCSS ve formě předdefinovaných dashboardů na základě konkrétní specifikace ze strany GFŘ.

2.3.7 Bezpečnostní monitoring

Bezpečnostní monitoring je zajištěn shromažďováním aplikačních bezpečnostních logů a bezpečnostních logů jednotlivých resource do Azure Log Analytics Workspace. Retence ukládaných dat je 31 dní. Z Log Analytics Workspace je možné následné zpracování a práce s bezpečnostními logy pomocí nástroje Azure Sentinel, na který je Log analytics workspace napojený. Z nástroje Azure Sentinel jsou zasílány alerty do SIEMu SPCSS.

2.4 Realizované činnosti

ID	Činnost	Zodpovědnost
1.	Ukončení a odstranění testovacího prostředí z MS Azure	SPCSS
2.	Odstranění zdrojů z produkčního prostředí	SPCSS

2.5 Požadovaná součinnost

Za účelem zajištění Služby poskytne Objednatel nezbytnou součinnost při:

3. předání seznamu určených osob pro plnění Služby Poskytovateli do 5ti dnů od zahájení poskytování Služby. Objednatel je povinen každou změnu určených osob prokazatelně ohlásit Poskytovateli. Požadavky v rámci Služby jsou Objednatelem zadávány pomocí Service Desku dle seznamu určených osob;
4. stanovení termínů odstávek;
5. využívání Service Desku za účelem zadání a řešení provozních požadavků a incidentů;
6. obnově certifikátů
7. požadavku na potřebnou součinnosti obou Smluvních stran, případně i jejich dodavatelů (třetích stran), jedna ze Smluvních stran požádá druhou Smluvní stranu o součinnost. Řízení součinností v rámci jednotlivých poskytovaných Služeb probíhá primárně prostřednictvím Service Desku nebo e-mailu.
8. aktualizaci operačních systémů (instalace patchů a security patchů) na základě doporučení výrobce nebo požadavků Objednatele, je prováděna na produkčním prostředí. Informace o plánované aktualizaci předává Poskytovatel minimálně tři pracovní dny předem prostřednictvím Service Desku nebo e-mailem na předem definované kontakty Objednatele. Tato informace bude obsahovat časový

harmonogram a dopady (i potenciální) do služby. Stejným způsobem proběhne informace po realizaci. Otestování funkčnosti aplikace je v zodpovědnosti Objednatele. Urgentní bezpečnostní záplaty jsou instalovány bez odkladu.

Dále:

9. Poskytovatel přidělí Objednateli nebo jeho dodavatelům potřebná přístupová oprávnění, která jsou nutná pro zajištění správy aplikace.

10. Poskytovatel poskytne Objednateli nebo jeho dodavatelům součinnost správce OS při činnostech vyžadujících oprávnění administrátora jako například:

10.1 Restarty serverů

10.2 Změny v registrech

10.3 Nastavení FW pravidel

11. V případě, že Objednatel trvá na převzetí administrátorských práv pak je Poskytovatel zodpovědný pouze za poskytování výpočetního výkonu nikoliv za provoz vlastního OS a dalších nadstavbových služeb.

Poskytovatel poskytne nezbytnou součinnost v případě ukončení služby:

12. při migraci provozu aplikací k jinému poskytovateli služeb

13. Součinnost musí být poskytnuta tak, aby nedošlo k ohrožení provozu portálů, jejichž hosting služba zajišťuje.

14. Poskytovatel zejména poskytne novému poskytovateli infrastruktury veškeré potřebné informace a umožní migraci dat, konfigurací, licencí i aplikací a bude spolupracovat s Objednatelem a třetími stranami tak, aby nedocházelo k zbytečným zpožděním, výpadkům a odstávkám.

15. Služba je poskytována a fakturována do akceptace migrace.

15.1 Dopady do kvalitativních parametrů poskytované Služby

15.1.1 Roční dostupnost Služby

Požadavek na roční dostupnost Služby podle tohoto Katalogového listu je uveden v následující tabulce:

Roční dostupnost			
v běžné provozní době		**v rozšířené provozní době**	
v %	**výpadek v hodinách**	**v %**	**výpadek v hodinách**
99,5	17 hod 30 min	98,0	105 hod 12 min

15.1.2 Požadované lhůty pro obnovení Služby

Požadavek na roční dostupnost Služby podle tohoto Katalogového listu je uveden v následující tabulce:

Lhůta pro obnovení Služby v běžné provozní době v hodinách		
Kritická závada	**Hlavní závada**	**Vedlejší závada**
4	6	24

15.1.3 Reakční doby Služby

Doba reakce úrovně L1 je počítána od zaevidování hlášení do aplikace Service Desk SPCSS (servicedesk.spcss.cz) (dále jen „Service Desk") dále . Podpora L1 musí do doby uvedené v tabulce níže přijmout v aplikaci Service Desk hlášení k řešení.

Požadavek na maximální dobu zahájení řešení incidentu v běžné provozní době v hodinách podle tohoto Katalogového listu je uveden v následující tabulce:

Maximální doba zahájení řešení incidentu v běžné provozní době v hodinách		
Kritická závada	**Hlavní závada**	**Vedlejší závada**
1	1	3

Poskytovatel je povinen závadu vyřešit v co nejkratším možném termínu, případně v termínu dle dohody s Objednatelem. Závada se považuje za vyřešenou jejím úplným vyřešením nebo alespoň uvedením do stavu Vedlejší závada (v případě závady Kritické nebo Hlavní), nedohodnou-li se smluvní strany jinak.

15.1.4 Kategorizace závad

Kritická	Služba není použitelná ve svých základních a klíčových funkcích, a přitom tato funkční závada znemožňuje jeho užívání většině nebo všem jejím uživatelům. Tento stav kritickým způsobem ohrožuje běžný provoz Objednatele v jeho klíčových procesech a aktivitách, případně způsobuje větší finanční nebo jiné kritické škody, a při tom neexistuje náhradní způsob zajištění poskytování služeb tohoto systému.
Hlavní	Služba je ve svých funkcích degradována tak, že tento stav zásadně omezuje běžný provoz Objednatele.
Vedlejší	Ostatní závady, které nespadají do závady Kritická nebo Hlavní.

15.1.5 Definice měření dostupnosti

Dostupnost Služby je definovaná jako splnění následující podmínky:

- webové portály www.etrzby.cz a epodpora.mfcr.cz jsou dostupné pro uživatele.

Za nahlášení nedostupnosti Služby se považuje okamžik založení odpovídajícího hlášení Objednatelem v aplikaci Service Desk nebo založení na základě automatického hlášení

incidentu dohledovým systémem Poskytovatele. Pro výpočet nedostupnosti jsou časy zaokrouhleny na celé minuty. Do doby nedostupnosti se započítávají všechny doby kritických závad včetně neplánovaných odstávek.

Dostupnost služby se vypočítá podle následujícího vzorce:

$$D = 100 \cdot \frac{T - N}{T}$$

kde

D	je dostupnost [%] v daném období
T	vyjadřuje fond provozní doby služby v daném období
N	vyjadřuje dobu v daném období, kdy byla služba nedostupná. Do doby nedostupnosti se nezapočítávají pravidelné odstávky a schválené mimořádné odstávky.

- Dostupnost je měřená ročně, a to od 00:00 hod. 1. 1. do 24:00 hod. 31. 12. každého kalendářního roku. Na počátku každého kalendářního roku Poskytovatel vypočítá maximální možné trvání nedostupnosti Služby pro dané období podle uvedených procentuálních hodnot požadované roční dostupnosti.
- Nedostupnost Služby v době schválených plánovaných a mimořádných odstávek se nezapočítává do celkové roční nedostupnosti Služby. Všechny tyto odstávky budou plánovány a následně odsouhlaseny Objednatelem.
- Do doby nedostupnosti se započítávají všechny doby trvání kritických závad včetně neplánovaných odstávek. Pokud byl incident způsoben prokazatelně mimo zodpovědnost Poskytovatele, do doby nedostupnosti se nezapočítává.
- Plánované odstávky jsou, pokud možno, soustředěny do servisních oken, která jsou každý čtvrtek v čase 19:00 až 24:00. Ve výjimečných případech jsou odstávky Služby oznamovány i mimo tato servisní okna. Ovlivnění chodu Služby ze strany Objednatele se nezapočítává do nedostupnosti Služby.

15.1.6 Nedodržení kvalitativního parametru Služby

V případě, že ze strany Poskytovatele dojde k nedodržení kvalitativního parametru Služby a pokud se Poskytovatel s Objednatelem nedohodnou jinak, Objednateli vzniká právo na uplatnění smluvní pokuty.

Poskytovatel bude zproštěn povinnosti dodržet kvalitativní parametr Služby, pokud:

- k nedostupnosti nebo závadě dojde ze strany Objednatele mimo působnost Poskytovatele ;

- k nedostupnosti nebo závadě dojde mimo infrastrukturu Poskytovatele (zejména v infrastruktuře GFŘ);
- vyskytnou se okolnosti, které představují událost vyšší moci.

15.2 Harmonogram realizace

Realizace proběhne dle schváleného harmonogramu.

15.3 Rizika

Pro produkční prostředí jsou tyto operace bez rizika, u testovacího je riziko pouze minimální v podobě budoucí potřeby tohoto prostředí. V tom případě bude nutné toto prostředí včetně všech nadstandardních konfigurací vybudovat znovu, což s sebou ponese riziko navýšení finančních zdrojů.

15.4 Cenové ohodnocení pracnosti a nákladů (pokud budou nad rámec Služby)

Bez dopadu do ceny služby.

15.5 Dopady do dokumentací

ID	Název	Popis změny
1.	Katalogový list GFŘ/005	Aktualizace

16. Společná sekce

Rozhodnutí

Datum	
Výsledek rozhodnutí	☒ Realizovat ☐ Nerealizovat ☐ Přepracovat ☐ Odložit
Podepsaná aktualizace smlouvy?	☐ Ano ☐ Ne ☒ Není potřeba

Podpisem oprávněné osoby potvrzujeme, že s návrhem změny výše popsané dle výsledku rozhodnutí souhlasíme. V případě výsledku Realizovat, je možné ihned zahájit práce na implementaci ZP.

V Praze dne (dle elektronického podpisu):

Objednatel	**Zhotovitel**
Jméno: [redacted]	Jméno: [redacted]
19.4.2023	17.4.2023
Podpis: _____	Podpis: _____
Jméno: [redacted]	Jméno: [redacted]
17.4.2023	04.04.2023
Podpis: _____	Podpis: _____