I3 Consultants s.r.o., K Trninám 645/34, 163 00 Praha

Dne: 12. září 2018

ČN: 12/2018

Gerontologické centrum v Praze 8
Šimůnkova 1600,
182 00 Praha 8 - Kobylisy

I3 Consultants

INGENIOSUS INTER INGENIOSI

NABÍDKA

"Zavedení systému ochrany osobních údajů dle GDPR"

1 Souhrn nabídky

1.1 Úvodem

Společnost I3 Consultants s.r.o. si dovoluje předložit nabídku na spolupráci při přechodu Vaší organizace do podmínek nové evropské legislativy (*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 volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů – General Data Protection Regulation)*, formou provedení „Zavedení systému ochrany osobních údajů dle GDPR".

V předložené nabídce je popsáno naše pochopení Vašich potřeb a současně náš přístup k jejich zajištění.

Nabízíme pouze ty služby, které jsme schopni plně garantovat a jejich kvalitu prokázat odpovídajícími referencemi, které přesně odpovídají poptávanému a současně nabízenému řešení.

1.2 Představení společnosti

1.2.1 Identifikační údaje

Obchodní název: I3 Consultants s.r.o.
Sídlo: K Trninám 945/34, 163 00 Praha 6 - Řepy
Adresa pobočky společnosti: Scheinerova 1570/6, 628 00 Brno
Tel./fax: +420 233 311 973
Mobil: +420 602 766 240
E-mail: info@i3c.cz
Statutární orgán: Ing. Tomáš Kubínek, jednatel; Ing. Igor Prosecký, jednatel
IČ: 279 21 344
DIČ: CZ 279 21 344
Zapsáno v obchodním rejstříku vedeného Městským soudem v Praze oddíl C, vložka 126634

1.2.2 Profil společnosti

I3 Consultants s.r.o. je konzultační a poradenskou společností, orientující se na poskytování služeb ve všech oblastech bezpečnosti informací s důrazem na oblast ochrany osobních údajů, kybernetické bezpečnosti a implementaci standardů ISMS a ITSM (ISO/IEC 27001 a 20000).

Společnost je držitelem:

- osvědčení podnikatele umožňující přístup k utajované informaci stupně utajení Důvěrné,
- certifikátu systému managementu kvality dle standardu ČSN EN ISO 9001:2009.

1.2.3 Reference a garance kvality

Vybrané referenční zakázky v oblasti bezpečnosti informací a ochrany osobních údajů:

<u>Ministerstvo práce a sociálních věcí ČR</u>

- ✓ zavedení jednotného systému řízení bezpečnosti informací v resortu - 2015

Ministerstvo životního prostředí ČR

- ✓ posouzení stávajícího stavu a zavedení systému ochrany osobních údajů – 2011
- ✓ Bezpečnostní politiky informací ministerstva - 2012

Ministerstvo pro místní rozvoj ČR

- ✓ posouzení stávajícího stavu a zavedení systému ochrany osobních údajů – 2011
- ✓ GAP analýza kybernetické bezpečnosti - 2015
- ✓ zajištění bezpečnostního dohledu MS 2014+ v oblasti řízení bezpečnosti informací a oblasti zpracování a ochrany osobních údajů – 2015 - dosud

Ministerstvo zemědělství ČR, sekce Pozemkové úřady

- ✓ ověření zavedeného systému zpracování osobních údajů a navržení jeho optimalizace, která zajistí plnou shodu zjištěných zpracování osobních údajů s požadavky zákona o ochraně osobních údajů – 2012

  Realizace projektu proběhla u všech 91 organizačních celků ve čtyřech na sobě navazujících etapách:
  - analýza současného stavu ochrany osobních údajů u ÚPÚ,
  - návrh optimalizace činností v oblasti ochrany osobních údajů, sumarizace výstupů z provedené analýzy,
  - implementace opatření zaměřených na optimalizaci systému ochrany osobních údajů,
  - zajištění akreditovaného školení pro zaměstnance ÚPÚ.

Ministerstvo kultury ČR

- ✓ provedení analýzy potřeb bezpečnostních služeb u Ministerstva kultury ČR a jím zřízených příspěvkových organizací, poradenských služeb v oblasti fyzické bezpečnosti při zadávání veřejné zakázky na poskytování bezpečnostních služeb v objektech Ministerstva kultury a jeho příspěvkových organizací a fondů 2012 - 2014
- ✓ posouzení stávající dokumentace ISMS s požadavky zákona o kybernetické bezpečnosti a vypracování nové dokumentace v souladu s požadavky zákona

Generální finanční ředitelství

- ✓ ustavení systému řízení bezpečnosti informací - 2014

Policejní prezidium České republiky – KB

- ✓ ustavení systému řízení bezpečnosti informací - 2016

Český statistický úřad

- ✓ srovnávací analýza souladu systémů s požadavky zákona o kybernetické bezpečnosti – 2015
- ✓ posouzení stávajícího stavu ochrany osobních údajů - 2015

Česká školní inspekce

- ✓ Validace akceptace, ISVS certifikace a implementace pravidel kybernetické bezpečnosti pro informační systém projektu NIQES - 2015
  - implementace požadavků souvisejících s legislativou vztahující se k oblasti kybernetické bezpečnosti, provozu ISVS a ochrany osobních údajů,
  - příprava informačních systémů veřejné správy k atestaci dle zákona č. 365/2000 Sb., včetně zpracování dokumentace,
  - provedení bezpečnostní prověrky s cílem ověřit shodu v oblasti kybernetické bezpečnosti,
  - provedení bezpečnostní prověrky s cílem ověřit shodu v oblasti ochrany osobních údajů - 2015.

Jihomoravský kraj – Krajský úřad Jihomoravského kraje

- ✓ posouzení stávajícího stavu a zavedení systému ochrany osobních údajů - 2008

Jihočeský kraj – Krajský úřad Jihočeského kraje
- ✓ posouzení stávajícího stavu a zavedení systému ochrany osobních údajů - 2015

Ústecký kraj – Krajský úřad Ústeckého kraje
- ✓ posouzení stávajícího stavu a zavedení systému ochrany osobních údajů - 2016

Zlínský kraj – Krajský úřad Zlínského kraje
- ✓ zpracování analýzy rizik a bezpečnostní dokumentace dle požadavků zákona o kybernetické bezpečnosti

Česká republika – Krajské státní zastupitelství Brno
- ✓ posouzení stávajícího stavu a zavedení systému ochrany osobních údajů - 2008
- ✓ ustavení systému řízení bezpečnosti informací – 2008

Česká republika – Krajský soud v Brně
- ✓ ustavení systému řízení bezpečnosti informací ISMS - 2014

Česká republika – Městský soud Praha, Městský soud v Brně, Okresní soud ve Žďáru nad Sázavou, v Kroměříži, v Blansku, v Hodoníně, ve Vyškově a další ...
- ✓ ustavení systému řízení bezpečnosti informací

Hlavní město Praha – Magistrát hlavního města Prahy – Odbor školství, mládeže a tělovýchovy
- ✓ posouzení stávajícího stavu a zavedení systému ochrany osobních údajů ve vybraných školách a školských zařízeních

Statutární město Brno – Magistrát města Brna, Městská policie Brno
- ✓ ustavení systému řízení bezpečnosti informací - 2011
- ✓ posouzení stávajícího stavu a zavedení systému ochrany osobních údajů – 2011
- ✓ outsourcing výkonu role Manažera bezpečnosti informací – 2012 - dosud

Statutární město Olomouc – Magistrát města Olomouc
- ✓ ustavení systému řízení bezpečnosti informací v rozsahu norem ISO 27000 a zákona o kybernetické bezpečnosti 2016 - 2017

Statutární město Kladno – Magistrát města Kladna
- ✓ posouzení stávajícího stavu a zavedení systému ochrany osobních údajů - 2009
- ✓ analýza rizik IS a vypracování návazné dokumentace - 2010

Statutární město Jihlava – Magistrát města Jihlavy
- ✓ posouzení stávajícího stavu a zavedení systému ochrany osobních údajů - 2010

Městský úřad Boskovice, Břeclav, Žďár nad Sázavou, Turnov, Uničov, Kyjov, Moravský Krumlov, Mikulov, Šumperk, Šternberk, Pohořelice a další ...
- ✓ posouzení stávajícího stavu a zavedení systému ochrany osobních údajů

Městská část Praha 1
- ✓ posouzení stávajícího stavu a zavedení systému ochrany osobních údajů - 2010

Městská část Praha 4
- ✓ posouzení stávajícího stavu a zavedení systému ochrany osobních údajů ve vybraných školách a školských zařízeních - 2014

Městská část Praha 5
- ✓ Aktualizace a konsolidace ISMS – 2013 - 2014
- ✓ posouzení současného stavu a zavedení systému ochrany osobních údajů 2013 - 2014
- ✓ posouzení stavu ochrany osobních údajů ve vybraných školách a školských zařízeních - 2013

Městská část Praha 12

- ✓ posouzení stávajícího stavu a zavedení systému ochrany osobních údajů ve vybraných školách a školských zařízeních - 2012

Městská část Praha 15

- ✓ posouzení stávajícího stavu a zavedení systému ochrany osobních údajů - 2012
- ✓ posouzení stávajícího stavu a zavedení systému ochrany osobních údajů ve vybraných školách a školských zařízeních - 2013

Fakultní nemocnice Ostrava

- ✓ provedení GAP analýzy požadavků zákona o kybernetické bezpečnosti (ZKB) - 2017
- ✓ provedení GAP analýzy požadavků nařízení Evropského parlamentu a Rady (EU) č. 910/2014 o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu (eIDAS) - 2017

Masarykův onkologický ústav Brno

- ✓ Ustavení systému řízení bezpečnosti informací – 2011
- ✓ posouzení současného stavu a zavedení systému ochrany osobních údajů - 2011

Fakultní nemocnice Plzeň

- ✓ Zpracování dokumentace pro ochranu osobních údajů v kamerovém systému včetně podkladů pro registraci - 2012

Fakultní nemocnice Ostrava

- ✓ zpracování návrhu strategie a koncepce bezpečnosti informací - 2011
- ✓ posouzení současného stavu a zavedení systému ochrany osobních údajů - 2011

Muzeum hl. m. Prahy

- ✓ posouzení současného stavu a zavedení systému ochrany osobních údajů – 2011

Unis a.s.

- ✓ ustavení systému řízení bezpečnosti informací – 2010
- ✓ zavedení systému managementu poskytování IT služeb (ITSM) - 2010

Unicontrols a.s.

- ✓ ustavení systému řízení bezpečnosti informací - 2017

Panasonic AVC Networks Czech, s.r.o.

- ✓ ustavení systému řízení bezpečnosti informací – 2012, analýza rizik - 2015
- ✓ posouzení současného stavu a zavedení systému ochrany osobních údajů - 2012

ČD-Telematika a.s.

- ✓ ustavení systému řízení bezpečnosti informací – 2010, aktualizace ISMS - 2015
- ✓ zavedení systému managementu poskytování IT služeb (ITSM) - 2010

Brněnské komunikace a.s.

- ✓ zavedení ISMS - 2015
- ✓ posouzení stávajícího stavu a zavedení systému ochrany osobních údajů – 2012
- ✓ zabezpečení činností v oblasti bezpečnosti informací a ochrany osobních údajů – 2012 - dosud

Dopravní podnik města Brna, a.s.

- ✓ ustavení systému řízení bezpečnosti informací - 2015
- ✓ posouzení současného stavu a zavedení systému ochrany osobních údajů - 2013
- ✓ příprava registrace vnitřního kamerového systému se záznamem pro dopravní prostředky DPMB – 2013 – 2015

Dopravní podnik hl. m. Prahy, akciová společnost

- ✓ Příprava registrace vnitřního kamerového systému se záznamem pro dopravní prostředky DPP – 2016

Dopravní společnost Zlín – Otrokovice, s.r.o.
- ✓ posouzení současného stavu a zavedení systému ochrany osobních údajů - 2011

Dopravní podnik města Jihlavy, a.s.
- ✓ posouzení současného stavu a zavedení systému ochrany osobních údajů - 2011

Plzeňské městské dopravní podniky, a.s.
- ✓ Příprava registrace vnitřního kamerového systému se záznamem pro dopravní prostředky PMDP, a.s. - 2014

Zdravotnická záchranná služba Jihomoravského kraje, p. o.
- ✓ posouzení stávajícího stavu a zavedení systému ochrany osobních údajů - 2013
- ✓ Příprava registrace kamerových systémů ZZS JmK - 2016

Tchibo ČR
- ✓ posouzení stávajícího stavu a zavedení systému ochrany osobních údajů – 2015

1.2.4 Reference ze zavedení systému ochrany osobních údajů dle GDPR

Liberecký kraj – Krajský úřad Libereckého kraje
- ✓ zavedení systému řízení bezpečnosti informací dle skupiny norem ČSN ISO/IEC 27000 a zákona č. 181/2014 Sb., o kybernetické bezpečnosti, včetně Nařízení Evropského parlamentu a Rady (EU) 2016/679 (GDPR)

Zlínský kraj – Krajský úřad Zlínského kraje
- ✓ Provedení vstupní a rozdílové analýzy požadavků GDPR a návrhů potřebných kroků pro dosažení souladu s GDPR pro Krajský úřad Zlínského kraje a pro příspěvkové organizace zřizované Zlínským krajem

Jihomoravský kraj – Krajský úřad Jihomoravského kraje
- ✓ Provedení vstupní a rozdílové analýzy stavu zpracování a ochrany osobních údajů a realizace kroků k uvedení do souladu s požadavky GDPR

Ministerstvo průmyslu a obchodu
- ✓ vypracování analýzy připravenosti na základě posouzení stavu ochrany osobních údajů ve vazbě na 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 volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (nařízení o ochraně osobních údajů - GDPR) ve vybraných státních podnicích v zakladatelské působnosti Ministerstva průmyslu a obchodu

Fakultní nemocnice Ostrava
- ✓ Provedení analýzy současného stavu zpracování a ochrany osobních údajů s cílem vytvořit výchozí podmínky pro implementaci obecného nařízení o ochraně osobních údajů (GDPR)

Nemocnice Vyškov
- ✓ provedení vstupní a GAP analýzy pro realizaci organizačních opatření k plnění požadavků vyplývajících z GDPR

Povodí Vltavy, státní podnik
- ✓ Provedení vstupní a rozdílové analýzy stavu zpracování a ochrany osobních údajů v souvislosti s přípravou k přechodu k GDPR, zpracování interních předpisů a potřebné související řídící dokumentace, včetně implementace systému OOÚ dle GDPR

Povodí Ohře, státní podnik
- ✓ implementace systému ochrany osobních údajů u objednatele, ve vztahu k Nařízení Evropského parlamentu a Rady (EU) 216/679 ze dne 27. dubna 2016

Město Jaroměř
- ✓ Implementace systému ochrany osobních údajů dle GDPR

Město Kroměříž
- ✓ vstupní a rozdílová analýza požadavků GDPR a návrhy potřebných kroků pro dosažení souladu s GDPR

Město Chropyně
- ✓ zavedení systému ochrany osobních údajů dle GDPR

Vojenské lesy a statky ČR, a.s.
- ✓ provedení vstupní a GAP analýzy pro realizaci organizačních opatření k plnění požadavků vyplývajících z GDPR

SITEL, spol. s r.o.
- ✓ Implementace systému ochrany osobních údajů dle GDPR

CENTRA a.s.
- ✓ Provedení vstupní a rozdílové analýzy stavu zpracování a ochrany osobních údajů v souvislosti s přípravou k přechodu k GDPR

X-TRADE BROKERS DOM MAKLERSKI SPóŁKA AKCYJNA, organizační složka
- ✓ Vstupní a rozdílové analýzy GDPR, včetně implementace procesů vedoucích k dosažení souladu s GDPR

Program Health Plus, s.r.o.
- ✓ Implementace požadavků GDPR

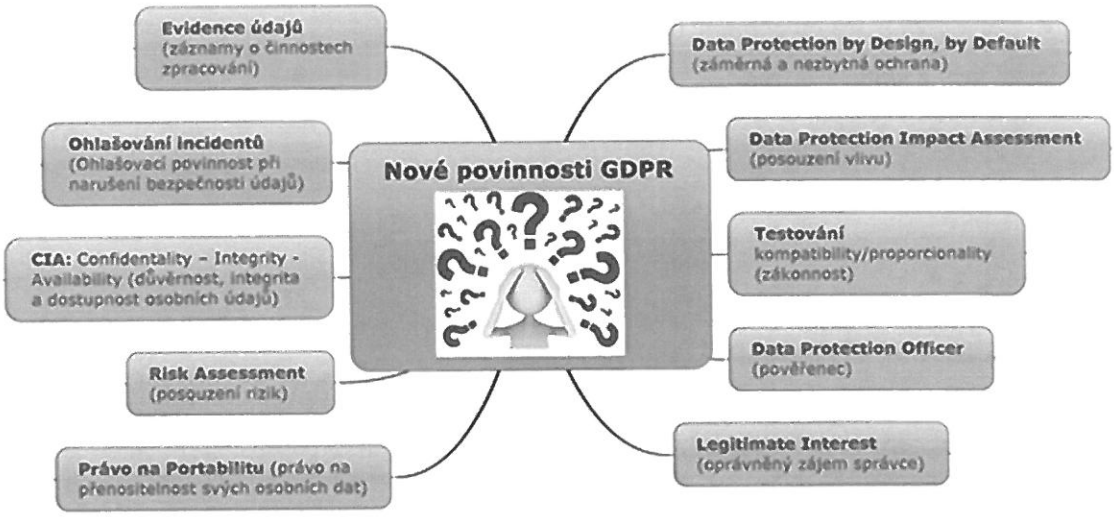
2 Informace ke změně legislativy při zpracování a ochraně osobních údajů

Pro sjednocení pravidel ochrany osobních údajů ve všech státech EU bylo dne 4. května 2016 v Úředním věstníku Evropské unie zveřejněno *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 volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů – General Data Protection Regulation)*, dále jen „*GDPR*".

GDPR bude účinné jednotně v členských zemích EU dnem 25. května 2018. V České republice tak nahradí současnou právní úpravu ochrany osobních údajů, tj. zákon č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů, ve znění pozdějších předpisů, kterým byly do národního prostředí transponovány povinnosti k ochraně osobních údajů vyplývající z již výše uvedené směrnice 95/46/ES.

GDPR představuje doposud nejucelenější soubor pravidel na ochranu dat. Nevyhnutně se dotkne každého, kdo shromažďuje nebo zpracovává osobní údaje obyvatel evropských zemí, a to včetně společností a institucí mimo území EU, které na evropském trhu působí. Je zřejmé, že všechny organizace musí reagovat na novou právní úpravu a budou muset upravit způsob zpracovávání osobních údajů.

GDPR rozvíjí a výrazně posiluje práva subjektů údajů (dotčených fyzických osob, kterým osobní údaje patří) s cílem zajistit možnost získat informaci o tom, které jejich údaje a z jakého důvodu jsou zpracovávány a současně mít možnost domáhat se dodržování stanovených pravidel, a to včetně nápravy stavu. Je tedy založeno na vymahatelnosti práv subjektů údajů a povinností správců (subjektů odpovědných za zpracování). Ve srovnání se stávajícím zákonem o ochraně osobních údajů stanovuje preciznější a propracovanější pravidla při zpracování osobních údajů a při jejich ochraně, což přináší zásadní změny a v určitých případech i úplně nová pravidla do stávajícího systému zpracování a ochrany osobních údajů.



Nově se každé organizace bude týkat celá řada změn a institutů, ke kterým patří zejména:

Data Protection by Design, by Default (záměrná a nezbytná ochrana)

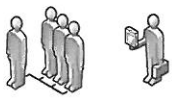
- ✓ implementace a zajištění prokazatelnosti **záměrné a nezbytné ochrany** („Data Protection by Design, by Default") osobních údajů zpracovávaných v listinné i elektronické podobě, a to ve všech fázích jejich životního cyklu,
  - **„by design"** – návrh vhodných technických a organizačních opatření již při **vývoji, návrhu, přípravě nebo tvorbě účelů a prostředků** zpracování,
  - **„by default" – technická a organizační opatření musí zajišťovat, aby byly zpracovávány pouze nezbytné údaje.**

Data Protection Impact Assessment (posouzení vlivu)

- ✓ nastavení nového způsobu spolupráce s dozorovým úřadem v závislosti na nutnosti provedení **posouzení vlivu** („Data Protection Impact Assessment") na ochranu osobních údajů u některých zpracování a případné vyžádání konzultace s dozorovým úřadem.

Testování kompatibility/proporcionality (zákonnost)

- ✓ nutnost provést u některých zamýšlených účelů zpracování **test** kompatibility/proporcionality s cílem posoudit zákonnost zpracování.



Data Protection Officer (pověřenec)

- ✓ povinnost jmenovat **pověřence pro ochranu osobních údajů** (Data Protection Officer – „DPO"), včetně zavedení všech procesů souvisejících s výkonem jeho působnosti.

Legitimate Interest (oprávněný zájem správce)

- ✓ možnost zpracovávat osobní údaje na základě „ **oprávněného zájmu** „ správce.

Souhlas (subjektu údajů, jako právní titul pro zpracování)

- ✓ nové aspekty pro udělení „souhlasu se zpracováním", vysoká pravděpodobnost **přeformulování** všech doposud udělených souhlasů s cílem získat schopnost doložit, že souhlas byl „Svobodný", „Konkrétní", „Informovaný", „Jednoznačný" a v případě zvláštních kategorií údajů „Výslovný".

Právo na Portabilitu (právo na přenositelnost svých osobních dat)

- ✓ možnost **„přenositelnosti"** osobních údajů, zpracovávaných automatizovaně, k jinému správci.

Risk Assessment (posouzení rizik)

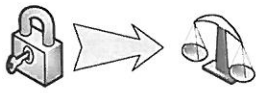
- ✓ provedení **analýzy/posouzení rizik** zpracování a ochrany osobních údajů, s cílem vyhodnotit závažnost zjištěných rizik a navrhnout opatření k jejich eliminaci,
- ✓ pro posouzení rizik lze využít standardizovaných metodik pro analýzu rizik dle ISO řady 31000 a 27000, je však nutné zohlednit další rizika jakými jsou např. riziko neoprávněného shromažďování, předávání atd.

CIA: Confidentality – Integrity - Availability (důvěrnost, integrita a dostupnost osobních údajů)

- ✓ zajištění případné **pseudonymizace** údajů u účelů zpracování, kde toto oddělení určitých informací může vést k vyšší záměrné či standardní ochraně osobních údajů,
- ✓ zajištění dalších opatření k ochraně osobních údajů formou např. **šifrování, minimalizací, obnovou dostupnosti nebo pravidelným testováním a hodnocením účinnosti** k ochraně

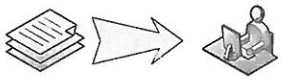
údajů se schopností odůvodnit, proč byla, respektive nebyla uplatněna výše uvedená opatření, doporučená GDPR,

- ✓ nastavení **politiky uchování a mazání dat** odpovídající uchování a likvidaci dat v listinné podobě – **ZÁSADNÍ PROBLÉM.**



Hlášení incidentů (Ohlašovací povinnost při narušení bezpečnosti údajů)

- ✓ nastavení procesu **ohlašovací povinnosti** v případě narušení bezpečnosti údajů dozorovému orgánu (v určitých případech i subjektu údajů) do časového limitu 72 hodin od okamžiku, kdy bylo toto narušení zjištěno.



Evidence údajů (záznamy o činnostech zpracování)

- ✓ zpracování **záznamů o činnostech** zpracování, které musí být zpracovány pro všechny existující účely zpracování (pokud nebude možné uplatnit výjimku z této povinnosti).

Zcela zásadní změnou je povinnost správce zajistit soulad přijatých a zdokumentovaných technických a organizačních opatření se všemi požadavky GDPR a současně být schopen je aktivně prokázat. Zákon č. 101/2000 Sb. tuto povinnost ukládal jen v rámci technickoorganizačních opatření k zajištění bezpečnosti osobních údajů (§ 13).

Další ze zásadních změn jsou i nepoměrně vyšší sankce za porušení ochrany osobních údajů, kdy oproti stávajícím téměř symbolickým sankcím ve výši do 10 mil. korun bude možno uložit sankce až do výše 20 mil. EUR.

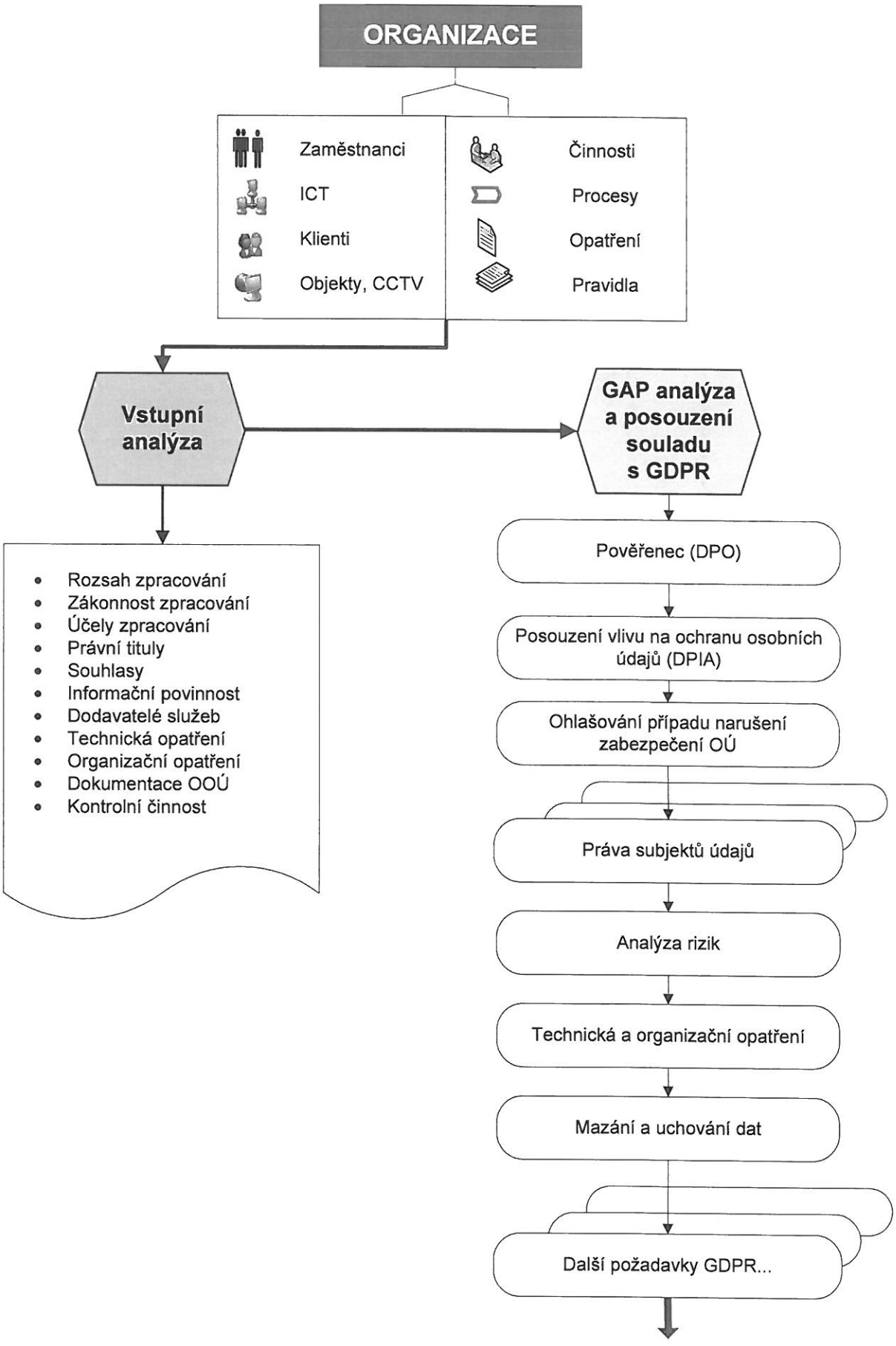
K přípravě na splnění požadavků GDPR je určeno období od dubna 2016, kdy GDPR vstoupilo v platnost, do května 2018, kdy GDPR nabude účinnosti.

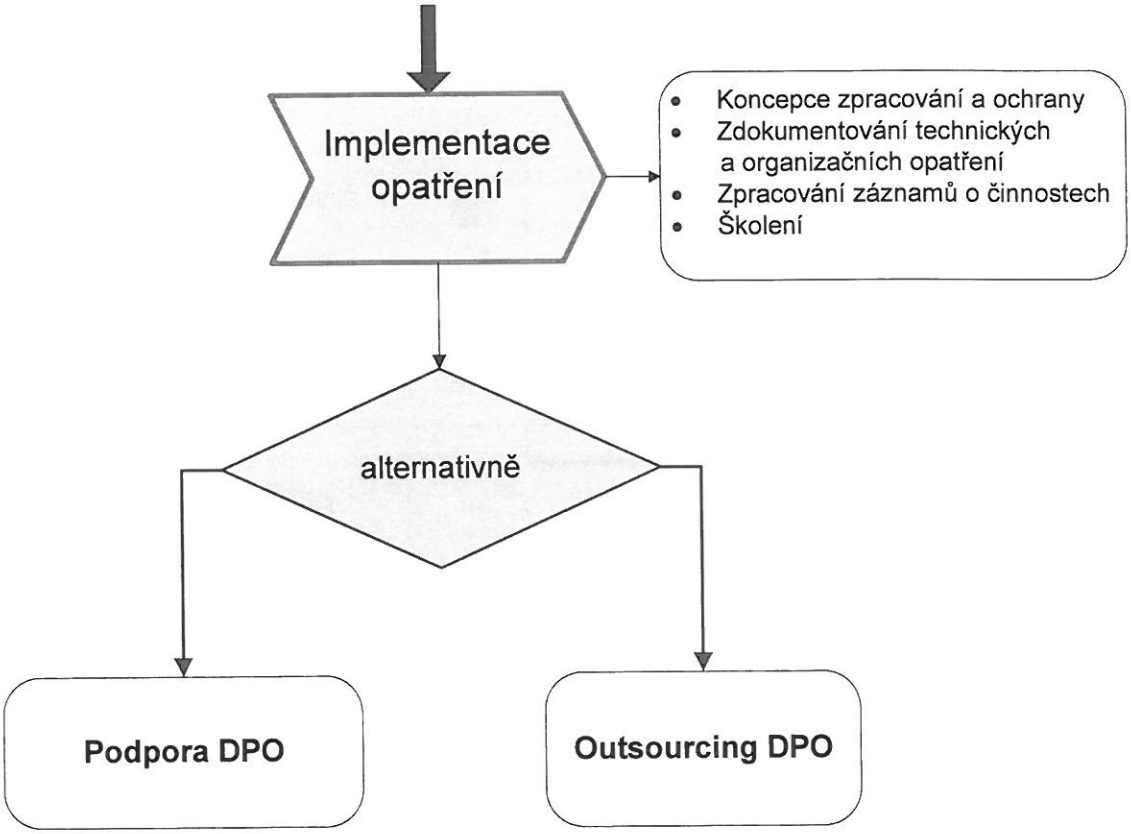
Je zřejmé, že GDPR bude mít značný dopad do stávajících procesů souvisejících se zpracováním a ochranou osobních údajů. Bude tedy nutné nejdříve zrevidovat stávající postupy nakládání s osobními údaji jak v listinné, tak i elektronické podobě a vyhodnotit rozsah zpracovávaných osobních údajů. Následně bude nutné porovnat zjištěný stav s požadavky GDPR a navrhnout potřebné změny a definice nových procesů způsobem, který zajistí prokazatelnost platnosti a dodržování stanovených pravidel po celou dobu zpracování osobních údajů.

Po provedení revize stávajícího stavu a návrhu definice změnových řízení bude nutné provést implementaci navržených a akceptovaných opatření do podmínek společnosti, což může představovat řadu nových či změněných technických, organizačních a procesních opatření.

Společnost I3 Consultants s.r.o. nabízí pomoc v následujících fázích přípravy a přechodu k GDPR, schematicky znázorněných v následujícím obrázku:

1) provedení revize (vstupní analýzy) stávajícího stavu zpracování a ochrany osobních údajů.
2) Provedení GAP analýzy a posouzení souladu s GDPR a návrh procesních, technických a organizačních opatření nutných pro zajištění souladu s GDPR.
3) Pomoc při implementaci technických a organizačních opatření.
4) Alternativně, na základě zjištěného stavu a reálných podmínek a potřeb objednatele, buď pravidelnou konzultační podporu výkonu role pověřence pro ochranu osobních údajů (DPO) nebo v určitých případech jeho outsourcing.


ORGANIZACE
Zaměstnanci
ICT
Klienti
Objekty, CCTV
Činnosti
Procesy
Opatření
Pravidla
Vstupní analýza
GAP analýza a posouzení souladu s GDPR
Rozsah zpracování
Zákonnost zpracování
Účely zpracování
Právní tituly
Souhlasy
Informační povinnost
Dodavatelé služeb
Technická opatření
Organizační opatření
Dokumentace OOÚ
Kontrolní činnost
Pověřenec (DPO)
Posouzení vlivu na ochranu osobních údajů (DPIA)
Ohlašování případu narušení zabezpečení OÚ
Práva subjektů údajů
Analýza rizik
Technická a organizační opatření
Mazání a uchování dat
Další požadavky GDPR...



3 Postup řešení

3.1 Etapa 1 – Vstupní analýza

Cílem etapy je zajistit a vyhodnotit zejména

1) Zjištění a vyhodnocení rozsahu a potřebnosti zpracování osobních údajů. V rámci tohoto kroku budou v součinnosti s objednatelem identifikovány jednotlivé účely zpracování osobních údajů.
2) Pro každý účel zpracování bude provedeno posouzení dodržení zásad zpracování dle článků 5 až 11 GDPR.
3) Bude posouzena prokazatelnost a kvalita souhlasů se zpracováním v případech, kdy zpracování osobních údajů podléhá souhlasu subjektu údajů a současně bude posouzeno plnění informační povinnosti podle článků 13 a 14 GDPR.
4) Posouzení smluvních vztahů s dodavateli služeb, kteří jsou zpracovateli ve smyslu článku 28 GDPR. V rámci tohoto kroku bude provedena:
    a) identifikace zpracovatelů,
    b) posouzení smluvních garancí zpracovatele k zajištění stanovené úrovně ochrany zpracování osobních údajů na základě smlouvy se správcem,
    c) identifikace případného řetězení zpracovatelů.

5) Posouzení rozsahu, efektivity a úrovně přijatých technických a organizačních opatření při zpracování osobních údajů s cílem vyhodnotit úroveň zajištění jejich důvěrnosti, integrity a dostupnosti. V rámci tohoto kroku bude ověřena:
    a) prokazatelnost a úroveň provedení analýzy rizik,
    b) opatření v oblasti počítačové, fyzické, personální, administrativní bezpečnosti,
    c) úroveň a rozsah realizace politiky uchování a mazání/likvidace dat, zpracovávaných automatizovaně i v listinné podobě.
6) Posouzení odpovědnosti za zapracování a ochranu osobních údajů v rámci objednatele.
7) Posouzení rozsahu a úrovně zpracované bezpečnostní dokumentace k ochraně osobních údajů.
8) Posouzení úrovně a rozsahu kontrolní činnosti směrem k zaměstnancům správce, zpracovatelům a dodavatelům.

3.2 Etapa 2 - Návrh procesních, technických a organizačních opatření nutných pro zajištění souladu s GDPR

Etapa 2 bude vycházet ze závěrů Etapy 1 a jejím cílem bude namapování všech požadavků GDPR na stávající stav zpracování a ochrany osobních údajů s cílem navrhnout potřebná změnová řízení a chybějící procesy, které povedou ke schopnosti prokázat soulad s principy a požadavky GDPR.

Výstupem bude návrh řešení chybějících procesních, organizačních a technických opatření, která zákon o ochraně osobních údajů nepožadoval a kterými jsou zejména:

1) Návrh jmenování pověřence pro ochranu osobních údajů (DPO).
2) Návrh katalogu/manuálu činností DPO, návrh jeho práv a povinností.
3) Návrh procesů k hlášení narušení bezpečnosti osobních údajů.
4) Návrh rozhodovacího procesu k uplatnění práva subjektů údajů.
5) Návrh rozhodovacího procesu pro realizaci posouzení vlivu na ochranu osobních údajů, včetně zpracování metodiky pro případné posouzení vlivu.
6) Návrh metodiky a postupu pro realizaci ochrany „by design".
7) Návrh metodiky a postupu pro realizaci ochrany „by default",
8) Návrh procesů k zajištění pravidelného testování a vyhodnocování účinnosti přijatých technických a organizačních opatření.

Následným výstupem Etapy 2 bude návrh potřebných změnových řízení, která odpovídajícím způsobem modifikují stávající procesní, technická a organizační opatření. Bude se jednat zejména o:

1) Úpravu formulace a rozsahu stávajících souhlasů subjektů údajů se zpracováním.
2) Revize a návrh úpravy informační povinnosti subjektům údajů.
3) Revize a návrh úpravy analýzy rizik.
4) V případě, že jsou zpracovávány citlivé údaje dle stávající terminologie zákona o ochraně osobních údajů, revize všech procesů souvisejících se zpracováním „zvláštní kategorie údajů" ve smyslu terminologie a požadavků GDPR.
5) Posouzení úrovně Politiky uchování a mazání dat.
6) Revize a návrh úprav procesů při uplatnění práv subjektů údajů.
7) Návrh úprav smluvních vztahů se Zpracovateli a Dodavateli služeb, v rámci kterých jsou zpracovávány osobní údaje.
8) Návrh úprav řešení kontrolní činnosti.

3.3 Návrh dokumentace k dosažení souladu s GDPR

Cílem této etapy je navrhnout konkrétní podobu chybějících procesů či změny současných a jejich zavedení pro praxe. Bude se jednat zejména o problematiku:

1) Provedení analýzy informačních rizik
2) Posouzení rizik se provádí analytickou metodou založenou na posuzování bezpečnostních charakteristik účelů zpracování z hlediska důvěrnosti integrity dostupnosti a kritičnosti daného zpracování OÚ a na jejich zobecnění do tzv. „typových účelů zpracování". Následně se posuzuje působení sady hrozeb, jejichž složení vychází jak z požadavků GDPR, tak z některých požadavků kybernetické bezpečnosti.
3) Výsledkem posouzení je stanovení nebezpečnosti jednotlivých hrozeb a sada doporučených opatření, u kterých je vyjádřena jejich efektivita působení, která se zohlední při plánování jejich implementace.
4) Analýza rizik se provádí softwarovým nástrojem společnosti I3 Consultants, s.r.o.
5) Vytvoření koncepce/politiky zpracování a ochrany osobních údajů, která umožní prokázat naplnění základních principů GDPR
6) Rozpracování koncepce/politiky ochrany osobních údajů do vnitřních předpisů a metodických pokynů organizace (správce).
7) Z pracování záznamů o činnostech zpracování pro identifikované účely zpracování v rozsahu stanoveném GDPR.

4 Nabídková cena

Etapa	Nabídková cena bez DPH
Etapa 1 – Vstupní analýza	48.000 Kč
Etapa 2 – Návrh procesních, technických a organizačních opatření nutných pro zajištění souladu s GDPR	20.000 Kč
Etapa 3 – Návrh dokumentace k dosažení souladu s GDPR	15.000 Kč

Nabídková cena je uvedena jako absolutní a nepřekročitelná částka za provedení celkové zakázky a obsahuje veškeré náklady se zakázkou spojené.

5 Doba plnění

Práce budou zahájeny v září 2018 a ukončeny do 30. 12. 2018.

6 Prohlášení o mlčenlivosti

Společnost I3 Consultants s.r.o. se tímto, a následně prostřednictvím smlouvy o dílo zavazuje, že neprozradí žádné třetí straně informace týkající se objednatele nebo souvisejících organizací, které se její zaměstnanci budou mít možnost dozvědět v souvislosti s prováděním služeb pro objednatele.

Společnost se zavazuje obeznámit všechny své zaměstnance se závazky zde a následně ve smlouvě učiněnými, a že učiní vše, aby jeho zaměstnanci dostáli těmto závazkům.

7 Závěr

Vážíme si skutečnosti, že jsme pro Vás mohli připravit tuto nabídku a věříme, že naše nabídka splňuje Vaše případné požadavky.

V případě nejasností či případných dalších požadavků nás prosím neváhejte kontaktovat.

Těšíme se na případnou spolupráci s Vámi.

Ing. Tomáš Kubínek
jednatel
I3 Consultants s.r.o.
K Trninám 945/34
163 00 Praha 6 - Řepy
Tel.:+420 233 311 973, Mobil: +420 602 766 240, www.i3c.cz