Magazín GDPR

číslo 1/2021

SOFT bit software

… Máme řešení i pro Vaši Společnost

www.softbit.cz

Vážení uživatelé našich informačních systémů,

pro všechny naše uživatele jsme připravili nové číslo našeho nepravidelného magazínu věnovaného tématice ochrany osobních údajů podle GDPR. Načerpali jsme další poznatky, které si myslíme, že budou pro Vás přínosné.

V řadě případů čerpáme přímo z informací uvolněných Úřadem pro ochranu osobních údajů doplněných o naše poznámky.

Věříme, že pro Vás informace, které získáte díky našemu dalšímu magazínu, budou užitečné při lepším zajištění procesů v ochraně osobních údajů ve Vaší organizaci podle GDPR.

Přejeme Vám příjemné čtení

Ing. Dana Peremská
pracovník zákaznické podpory

Obsah magazínu

Osobní údaje zaměstnance – jak je zpracovávat

Zaměstnavatelé dávají v mnoha případ podepsat svým zaměstnancům souhlas se zpracováním osobních údajů s velmi obecnými formulacemi a domnívají se, že podpisem takového souhlasu mají ošetřeno nakládání s osobními údaji zaměstnanců a nemusí činit již další kroky. **Tento přístup je však velmi špatný.**

Zaměstnavatel by neměl vyžadovat souhlas zaměstnance se zpracováním údajů, pokud je schopen identifikovat a prokázat, že osobní údaje zaměstnance zpracovává na základě jiného důvodu (např. plnění smlouvy uzavřené se zaměstnancem). **Souhlas se zpracováním osobních údajů ze strany zaměstnance by měl být využit až jako poslední důvod ke zpracování v případě, že se neuplatní důvod jiný.**

Případy, kdy je zaměstnavatel oprávněn či povinen zpracovávat osobní údaje svých zaměstnanců:

- ✓ zaměstnanec udělil souhlas ke zpracování osobních údajů
- ✓ zpracování osobních údajů je nezbytné k plnění smlouvy uzavřené se zaměstnancem (pracovní smlouva, DPČ, DPP)
- ✓ zpracování je nezbytné k plnění právní povinnosti zaměstnavatele
- ✓ zpracování je nezbytné pro ochranu životně důležitých zájmů zaměstnance
- ✓ zpracování je nezbytné pro plnění úkolů ve veřejném zájmu nebo při výkonu veřejné moci, kterým byl správce pověřen
- ✓ zpracování je nezbytné pro účely oprávněných zájmů zaměstnavatele

Pokud zaměstnavatel není schopen zařadit zpracování osobních údajů pod žádný zvýše uvedených případů, není oprávněn tyto údaje dále zpracovávat.

Souhlas v separátním dokumentu

Jestliže je nezbytné zpracovávat osobní údaje zaměstnance na základě jeho souhlasu, mělo by toto být uvedeno v separátním dokumentu. **Daný souhlas by neměl být součástí pracovní či jiné smlouvy,** ani by neměl být uveden ve všeobecných nebo jiných obchodních podmínkách.

Plnění smlouvy

Na základě plnění smlouvy zaměstnavatel zpracovává **identifikační údaje** zaměstnance (např. jméno, příjmení, datum narození, adresu, atd.). Kromě těchto údajů však zpracovává i např. **číslo bankovního účtu** z důvodu výplaty mzdy, **identifikaci zdravotní pojišťovny** zaměstnance pro účely zákonných odvodů záloh, **počet dětí** z důvodu plnění povinností stanovených daňovými předpisy apod. **Všechny tyto osobní údaje zpracovává zaměstnavatel v souvislosti s plněním smlouvy nebo jiných právních povinností.** Zpracovávat osobní údaje zaměstnance spojené se srážkami ze mzdy v případě výkonu rozhodnutí nebo exekuce se řídí zvláštními právními předpisy týkající se srážek ze mzdy na základě rozhodnutí soudu či exekutora. K takovým to osobním údajům není tedy třeba souhlas zaměstnance se zpracováním údajů.

Výčet osobních údajů zaměstnance zpracovávaných zaměstnavatelem jakožto správcem závisí na postavení zaměstnance k zaměstnavateli. Toto postavení se v průběhu času může měnit. Jiné osobní údaje bude zaměstnavatel o zaměstnanci zpracovávat v průběhu výběrového řízení, jiné za trvání pracovního poměru a jiné po skončení pracovního poměru. Dále také závisí na povaze práce, jiné osobní údaje bude zaměstnavatel zpracovávat o pokladní v supermarketu a jiné o provozním řediteli tohoto supermarketu.

Výběrové řízení a zpracování osobních údajů

Při výběrovém řízení se do rukou zaměstnavatele dostávají osobní údaje potencionálního zaměstnance, jako je např. jméno, příjmení, adresa, telefon, e-mail, dosažené vzdělání, kvalifikace, pracovní zkušenosti atd. **Zaměstnavatel je povinen nakládat se všemi těmito údaji jako s osobními údaji. Se zpracováním těchto údajů není potřeba vyžadovat od potencionálního zaměstnance souhlas,** neboť tyto údaje se uchovávají v rámci jednání směřujícího k uzavření pracovní či jiné smlouvy. Zaměstnavatel také nemusí o zpracování údajů pro účely výběrového řízení ani informovat.

Pokud se zaměstnavatel rozhodne, že potencionálního zaměstnance nepřijme, **neměl by jeho osobní údaje vůbec uchovávat a dále zpracovávat. Pro případ podání stížnosti od uchazeče na nepřijetí se doporučuje jeho osobní údaje zpracovávat.** Zaměstnavatel je pak schopen prokázat, z jakého důvodu nebyl uchazeč přijat.

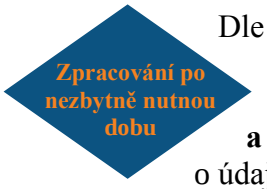
Příkladem je požadavek nepřijatého uchazeče na odškodném od zaměstnavatele za nepřijetí z důvodu diskriminace. V takovém případě by zaměstnavatel mohl prokázat nepřijetí uchazeče např. z důvodu nedostatečného vzdělání potřebného pro danou pozici.

Zaměstnavatel uchazeče nepřijme, ale chce zpracovávat jeho osobní údaje pro účely možného oslovení v budoucnu. Tento případ je velmi diskutabilní, **doporučujeme požádat uchazeče o udělení souhlasu ke zpracování osobních údajů.**

Vznik pracovního poměru a zpracování osobních údajů

Při vzniku pracovního poměru zaměstnavatel se zaměstnancem uzavírá pracovní či jiné smlouvy. **Zaměstnavatel musí informovat zaměstnance o zpracování jeho osobních údajů**, ideálně při podpisu pracovní smlouvy. Ve většině případů zpracovává zaměstnavatel osobní údaje zaměstnance na základě plnění povinností plynoucích z pracovní či jiné smlouvy, případně na základě oprávněných zájmů zaměstnavatele.

Skončení pracovního poměru a zpracování osobních údajů



Dle základních zásad GDPR, by zpracování osobních údajů mělo probíhat pouze po nezbytně nutnou dobu. Po ukončení pracovního poměru (je jedno zda pracovní poměr ukončí zaměstnanec nebo zaměstnavatel), by zaměstnavatel **nadále neměl uchovávat a zpracovávat osobní údaje zaměstnance, které již nepotřebuje.** Jedná se především o údaje vztahující se k personální a mzdové agendě zaměstnance. Pro případné budoucí spory s bývalým **zaměstnancem se doporučuje zpracovávat** i tyto osobní údaje, doba zpracování by však neměla přesáhnout tři roky.

Příkladem je ukončení pracovního poměru ze strany zaměstnavatele z důvodu opakovaného porušování doby docházky. V takovém případě se zaměstnavatel může prokázat údaji o docházce zaměstnance, které jsou však také osobními údaji.

Souhlas zákazníka se zpracováním osobních údajů

Souhlas zákazníka se zpracováním osobních údajů musí být výslovný, vědomý a svobodný. Správce osobních údajů musí být schopen prokázat, že subjekt údajů projevil souhlas se zpracováním svých osobních údajů aktivním jednáním a předem získal informace o všech okolnostech souvisejících se zpracováním těchto údajů ve srozumitelné a snadno přístupné formě. Informace musí být poskytnuty v jasném a jednoduchém jazyce, který umožňuje jednoduše rozpoznat důsledky daného souhlasu. Pole pro udělení souhlasu zákazníka nesmí být automaticky předem zaškrtnuto.

Jestliže je souhlas subjektu údajů se zpracováním osobních údajů vyjádřen písemným prohlášením, které se týká i jiných skutečností, musí být žádost o vyjádření souhlasu předložena jasně odlišitelným způsobem od těchto jiných skutečností. Dané prohlášení musí být srozumitelné a snadno přístupné za použití jasného a jednoduchého jazyka.

Pro zajištění skutečné svobodné volby zákazníka nesmí smluvní ujednání uvádět subjekt údaj v omyl, pokud jde o možnost uzavření smlouvy, i přes odmítnutí zákazníka souhlasit se zpracováním svých údajů.

Registrační značka jako osobní údaj

Registrační značka se nevztahuje k vozidlu, ale k jeho vlastníkovi či provozovateli. Z obsahu registru vozidel zřetelně vyplývá, že v daný okamžik je vozidlo (i registrační značka) spojeno s konkrétním vlastníkem či provozovatelem, který je nepřímo identifikovatelný prostřednictvím daného vozidla. V případě, že je vlastník či provozovatel fyzickou osobou, je identifikovatelný na základě registrační značky z důvodu zápisu jeho údajů do registru vozidel. V takovém případě je registrační značka osobním údajem.

Pokud se však registrační značka nevztahuje ke konkrétní fyzické osobě vlastníka či provozovatele, nejedná se o osobní údaj.

Definice osobního údaje - čl. 4 bod 1) GDPR

Osobními údaji jsou veškeré informace o identifikované nebo identifikovatelné fyzické osobě. Identifikovatelnou fyzickou osobou je fyzická osoba, kterou lze přímo či nepřímo identifikovat, zejména odkazem na určitý identifikátor, například jméno, identifikační číslo, lokační údaje, síťový identifikátor nebo na jeden či více zvláštních prvků fyzické fyziologické, genetické, psychické, ekonomické, kulturní nebo společenské identity této fyzické osoby.

Videokonference – ochrana osobních údajů

Pro zpracování osobních údajů osob účastnících se videokonferencí je třeba se řídit ustanovením čl. 6 odst. 1 písm. a), b), e), f) GDPR, případně také zákonem č. 110/2019 Sb., o zpracování osobních údajů. **Zpracování těchto osobních údajů může být založeno na uděleném, dobrovolném a informovaném souhlasu (dle čl. 4 a bod 11 GDPR).** Dobrovolnou účast lze předpokládat pouze tehdy, jestliže k účasti na videokonferenci existuje reálná alternativa. Pokud tato alternativa neexistuje v rámci plnění smlouvy dle čl. 6 odst. 1 písm. b) GDPR, nebo se videokonference účastní zaměstnanci jiných společností a jiných osob, zpracování osobních údajů může legitimizovat oprávněný zájem dle č. 6 odst. 1 písm. f) GDPR. V tomto případě však musí odpovědná osoba informovat účastníky konference o právu vznést námitku v souladu s čl. 21 odst. 4 GDPR.

Orgány státní správy se však řídí čl. 6 odst. 1 písm. e) GDPR v souvislosti s příslušnou normou českého práva (např. školský zákon).

Zaměstnavatel jako odpovědná osoba

Jestliže je osobou odpovědnou za ochranu osobních údajů zaměstnavatel, na jehož pokyn zaměstnanci používají videokonferenční systém za účelem plnění svých smluvních a pracovních povinností, je právní základ pro zpracování údajů založen na zákoníku práce. Je nutné však vždy zkontrolovat nutnost přenosu obrazových dat. Nikdy nesmí být podhodnocena úroveň ochrany GDPR.

Odpovědná osoba musí být vždy schopna prokázat, že dodržuje zásady ochrany osobních údajů, a to dle čl. 5 odst. 2 GDPR.

Údaje o zdraví, náboženská výchova apod.

Pokud se během videokonference projednávají např. údaje o zdraví a zdravotní stav, nebo se jedná o náboženskou výchovu, teologická studia atd. je potřeba se řídit čl. 9 odst. 2 GDPR. V takovém případě může být vyžadován samostatný **souhlas účastníka, ten však musí být informovaný, dobrovolný, předchozí, aktivní, jednoznačný pro konkrétní případ, samostatně deklarovaný a kdykoli přiměřeně odvolatelný.**

Čl. 9 odst. 1 GDPR

Zakazuje se zpracování osobních údajů, které vypovídají o rasovém či etnickém původu, politických názorech, náboženském vyznání či filozofickém přesvědčení nebo členství v odborech, a zpracování genetických údajů, biometrických údajů za účelem jedinečné identifikace fyzické osoby a údajů o zdravotním stavu či o sexuálním životě nebo sexuální orientaci fyzické osoby.

Videokonference z domova

Při účasti zaměstnanců videokonference z domova vzniká zásah do soukromí ostatních účastníků bez jejich souhlasu, a to prostřednictvím obrazu nebo zvuku. **Zaměstnavatel tedy musí provést technická a organizační opatření dle čl. 25 odst. 1 GDPR,** např. vyrovnání kamery, aktivace virtuálního pozadí apod.

Čl. 25 odst. 1 GDPR

S přihlédnutím ke stavu techniky, nákladům na provedení, povaze, rozsahu, kontextu a účelům zpracování i různě pravděpodobným a různě závažným rizikům pro práva a svobody fyzických osob, jež s sebou zpracování nese, zavede správce jak v době určení prostředků pro zpracování, tak v době zpracování samotného vhodná technická a organizační opatření, jako je pseudonymizace, jejichž účelem je provádět zásady ochrany údajů, jako je minimalizace údajů, účinným způsobem a začlenit do zpracování nezbytné záruky, tak aby splnit požadavky tohoto nařízení a ochránil práva subjektů údajů.

Jako alternativu k těmto technickým a organizačním opatřením lze použít souhlas zaměstnanců, ten by však musel být dobrovolný, což je vzhledem k pracovněprávnímu vztahu značně problematické.

Poskytovatel služeb – zpracování údajů

Poskytovatel videokonferenčních služeb se nemůže při zpracovávání osobních údajů pro své vlastní účely řídit právním základem, kterým se řídí organizátor konference.

Dle čl. 5 odst. 1 písm. b) GDPR musí být osobní údaje shromažďovány pro určité, výslovně vyjádřené a legitimní účely a nesmějí být dále zpracovávány způsobem, který je s těmito účely neslučitelný; další zpracování pro účely archivace ve veřejném zájmu, pro účely vědeckého či historického výzkumu nebo pro statistické účely se podle čl. 89 odst. 1 nepovažuje za neslučitelné s původními účely.

Zpracovatel musí uvést ve smlouvě o zpracování osobních údajů, že zpracovává osobní údaje zúčastněných osob pouze na pokyny odpovědné osoby a nikoli pro vlastní účely.

Zpracování údajů třetích osob

Musí být zajištěna transparentnost

Pro zpracování osobních údajů třetích osob, které se neúčastní videokonference, ale jejich osobní údaje jsou ve videokonference diskutovány, se použijí obecné právní základy. **Dále musí být jasně definován druh a účel zpracování osobních údajů, pro splnění požadavků na transparentnost dle čl. 12 GDPR.** Pro zajištění transparentnosti musí také být informace prezentovány tak, aby jim průměrný uživatel služby rozuměl bez zbytečného úsilí. Je třeba se vyvarovat příliš složitých jazykových, technických nebo právních výrazů. Jestliže je nutné použít technické výrazy, musí být vysvětleny srozumitelným způsobem.

Povinnosti organizátora videokonference

Organizátor je odpovědný za zpracování údajů

Organizátor videokonference je při provozu či používání této služby odpovědný za zpracování osobních údajů a musí splnit povinnosti podle GDPR.

Zodpovědné osoby musí osobám účastnícím se videokonference poskytnout jasné a jednoznačné informace o zpracování osobních údajů souvisejících s využíváním služby v souladu s čl. 13 a 14 GDPR.

Především se jedná o tyto informace:

- ✓ účel zpracování osobních údajů
- ✓ na jakém právním základě se osobní údaje zpracovávají
- ✓ po jakou dobu jsou údaje uchovávány po ukončení konference
- ✓ zda mohou být údaje předány do třetí země
- ✓ typ šifrování, který se při provozu služby použije
- ✓ zda může organizátor videokonferenci nahrát a uložit **(Účastníci musí být informováni o probíhajícím záznamu, pokud je aktivována funkce nahrávání)**
- ✓ jaké operace zpracování údajů jsou založeny na souhlasu zúčastněných osob

U operací zpracování údajů založených na souhlasu nesmí docházet k nedostatečné informovanosti účastníků videokonference, jelikož by tak mohlo dojít k nezákonnosti zpracování údajů.

Organizátor videokonference by měl dále informovat účastníky o možnostech úpravy nastavení aplikace (např. použití pseudonymu, nastavení virtuálního pozadí atd.).

Přenos osobních údajů do třetích zemí

V případě videokonferenčních systémů, které přenášejí data do třetích zemí (do zemí mimo EU nebo do Evropského hospodářského prostoru), musí přenos odpovídat zvláštním podmínkám. K takovýmto převodům může dojít zejména u poskytovatelů se sídlem ve třetích zemích nebo využívajících subdodavatele ze třetích zemí.

Na poskytovatele videokonferenčních systémů mimo území EU se vztahuje nařízení za podmínek stanovených v čl. 3 odst. 2 GDPR a dále také zákonná ustanovení jejich domovské země.

Evropská komise rozhodla, že v některých třetích zemích existuje odpovídající úroveň ochrany údajů a v takových případech nemusí být tedy splněny žádné další podmínky pro přípustnost přenosu osobních údajů, viz čl. 45 GDPR.

Podmínky pro přenos mohou být také dodrženy prostřednictvím standardních smluvních doložek Komise EU, které správce uzavírá s poskytovatelem jako zpracovatelem.

Pokud dochází k přenosu dat do třetích zemí, musí odpovědné osoby zkontrolovat, zda zvolené nástroje předávání zaručují používání daných osobních údajů se stejnou ochranou během přenosu i v samotné třetí zemi jako v EU, případně přijmou další opatření k zajištění dané ochrany. Osoby odpovědné za používání videokonferenčních služeb musí být schopny prokázat, že provedly tuto kontrolu a údaje ve třetí zemi jsou tedy odpovídajícím způsobem chráněny a v souladu s danými normami, viz čl. 5 odst. 2 GDPR.

Nejhorší hesla roku 2020

Správce osobních údajů by měl své zaměstnance pravidelně upozorňovat, jaké jsou nejčastější chyby při vytváření hesla a jak bezpečné heslo vytvořit. V tomto článku se dočtete základní pravidla pro bezpečné heslo, jak vytvořit silné heslo a jaká byla nejhorší hesla v roce 2020.

Základní pravidla pro bezpečné heslo

- ✓ **Nepoužívání stejných hesel pro více účtů či zařízení** (pro každý účet nebo zařízení doporučujeme vytvořit jedinečné a složité heslo). Stejné heslo pro více účtů je jako mít stejný klíč ke svému autu, kanceláři a bytu.
- ✓ **Nepoužívání snadno zapamatovatelných hesel.** Snadné heslo je vytvořeno podle jmen rodinných příslušníků a přátel, názvů sportů, filmů, seriálů, knih, jmen postav, nadávek, řady po sobě jdoucích čísel či písmen (např. „qwerty“, „123456“), opakující se znaky (např. „aaaa“, „123abc“) osobní údaje (např. telefonní číslo, datum narození, jméno, adresa). Používat snadno zapamatovatelná hesla je horší než si hesla napsat na papír.
- ✓ **Nepoužívání krátkých hesel** (doporučujeme heslo o délce minimálně 12 znaků).
- ✓ **Doporučujeme kombinace** velkých a malých písmen, písmen s háčky, dlouhé hlásky, čísla a speciální znaky.
- ✓ **Nepoužívání běžně nahraditelných znaků** (např. hesla „INTERNET“ a „1NT3RN3T“ jsou obě stejně snadno prolomitelná).
- ✓ **Změňte heslo alespoň každých 90 dní.** Pravidelná změna je náročná na zapamatování, ve většině případů tak dochází ke snižování kvality hesla. Nestačí pouze změnit jedno písmeno nebo přidat číslo k již používanému heslu. V tomto případě doporučujeme používat jedno složité a těžko prolomitelné heslo celý rok, než během jednoho roku vystřídat šest jednoduchých hesel.
- ✓ **Doporučujeme používat dvoustupňové** (vícestupňové) **ověření.**

Společnost NordPass každý rok sestavuje žebříček 200 nejčastějších hesel za celý rok. Žebříček udává, kolik uživatelů toto heslo používá a kolik času by trvalo jeho prolomení. Společnost také porovnává nejhorší hesla za rok 2019 a 2020 a jak se změnila jejich pozice (zelená šipka značí vzrůst a červená šipka úpadek). **Na další stránce tohoto magazínu Vám uvádíme výčet 50 nejčastějších hesel za rok 2020.** Celý seznam 200 nejčastějších hesel v loňském roce si můžete prohlédnout na stránce společnosti NordPass **zde.**

Top 50 nejčastějších hesel roku 2020			
Pozice	Heslo	Počet uživatelů	Čas prolomení
1. ↑ (2)	**123456**	2 543 285	Méně než 1 sekunda
2. ↑ (3)	**123456789**	961 435	Méně než 1 sekunda
3. (nové)	**picture1**	371 612	3 hodiny
4. ↑ (5)	**password**	360 467	Méně než 1 sekunda
5. ↑ (6)	**12345678**	322 187	Méně než 1 sekunda
6. ↑ (17)	**111111**	230 507	Méně než 1 sekunda
7. ↑ (18)	**123123**	189 327	Méně než 1 sekunda
8. ↓ (1)	**12345**	188 268	Méně než 1 sekunda
9. ↑ (11)	**1234567890**	171 724	Méně než 1 sekunda
10. (nové)	**senha**	167 728	10 sekund
11. ↑ (12)	**1234567**	165 909	Méně než 1 sekunda
12. ↓ (10)	**qwerty**	156 765	Méně než 1 sekunda
13. ↑ (16)	**abc123**	151 804	Méně než 1 sekunda
14. (nové)	**Million2**	143 664	3 hodiny
15. ↑ (28)	**000000**	122 982	Méně než 1 sekunda
16. ↓ (15)	**1234**	112 297	Méně než 1 sekunda
17. ↓ (14)	**iloveyou**	106 327	Méně než 1 sekunda
18. (nové)	**aaron431**	90 256	3 hodiny
19. ↑ (29)	**password1**	87 556	Méně než 1 sekunda
20. (nové)	**qqww1122**	85 476	52 minut
21. ↑ (199)	**123**	84 438	Méně než 1 sekunda
22. (nové)	**omgpop**	77 492	2 minuty
23. ↑ (39)	**123321**	73 506	Méně než 1 sekunda
24. ↑ (36)	**654321**	69 148	Méně než 1 sekunda
25. ↓ (22)	**qwertyuiop**	64 632	Méně než 1 sekunda
26. (nové)	**qwer123456**	58 096	4 sekundy
27. ↑ (158)	**123456a**	57 472	Méně než 1 sekunda
28. ↑ (197)	**a123456**	55 548	Méně než 1 sekunda
29. ↑ (57)	**666666**	53 146	Méně než 1 sekunda
30. ↑ (35)	**asdfghjkl**	52 961	Méně než 1 sekunda
31. ↓ (26)	**ashley**	52 031	2 minuty
32. ↑ (58)	**987654321**	50 097	Méně než 1 sekunda
33. (nové)	**unknown**	47 995	17 minut
34. ↑ (65)	**zxcvbnm**	46 952	Méně než 1 sekunda
35. ↑ (54)	**112233**	46 450	Méně než 1 sekunda
36. (nové)	**chatbooks**	45 883	1 den
37. (nové)	**20100728**	44 914	Méně než 1 sekunda
38. ↑ (147)	**123123123**	42 781	Méně než 1 sekunda
39. ↓ (21)	**princess**	42 230	Méně než 1 sekunda
40. (nové)	**jacket025**	41 909	8 hodin
41. (nové)	**evite**	41 720	10 sekund
42. ↑ (122)	**123abc**	40 431	Méně než 1 sekunda
43. ↑ (111)	**123qwe**	40 203	Méně než 1 sekunda
44. ↓ (23)	**sunshine**	39 456	Méně než 1 sekunda
45. ↑ (67)	**121212**	39 342	Méně než 1 sekunda
46. ↑ (70)	**dragon**	39 011	Méně než 1 sekunda
47. ↑ (104)	**1q2w3e4r**	38 865	Méně než 1 sekunda
48. (nové)	**5201314**	38 307	26 sekund
49. ↑ (168)	**159753**	38 028	Méně než 1 sekunda
50. ↓ (3)	**0123456789**	37 280	Méně než 1 sekunda

Zajímavá fakta z výzkumu nejčastěji používaných hesel

- ✓ 78 hesel se v tomto žebříčku objevilo poprvé.
- ✓ heslo „onedirection“ – v loňském roce bylo toto heslo na 184. pozici. V letošním roce se toto heslo v žebříčku nejčastějších hesel vůbec neobjevilo. Z těchto údajů lze zjistit, že hudební kapela Onedirection ztrácí popularitu, jelikož se její členové věnují sólové kariéře nebo si jejich fanoušci více uvědomují nebezpečí snadných hesel.

Zdroj: NordPass

Nabídka základních služeb GDPR

Naší prioritou je dodávat našim zákazníkům kompletní služby. Z tohoto důvodu naše společnost rozšířila v roce 2017 nabídku o poskytování služeb v oblasti správy a ochrany osobních údajů. V současné době naše služby v této oblasti využívá více jak 100 zákazníků z různých oblastí státní správy i podnikatelského světa.

Rádi Vám umíme nabídnout:

- ✓ Zpracování úvodního vnitřního auditu k evidenci, uchovávání a zabezpečení veškerých informací o fyzických osobách, a to jak v elektronické, tak i v listinné podobě.
- ✓ Na základě tohoto auditu je zpracována vnitropodniková směrnice k nakládání s osobními údaji podle nařízení GDPR, která popisuje jednotlivé části v informačních systémech a evidenci dokumentů ve Vaší společnosti a navrhujeme taková řešení, která povedou k zajištění vyšší bezpečnosti dat o fyzických osobách.
- ✓ Toto by měl být začátek naší spolupráce. Doporučujeme revizi vnitropodnikové směrnice vždy za určité období (ideální rok), kdy se provedou inventarizace změn proti předchozímu období a vyhodnotí se provedené změny.
- ✓ Školení všech pracovníků společnosti, kteří přicházejí do styku s osobními údaji subjektu údajů.
- ✓ S každým klientem k tomuto uzavíráme smlouvu pro služby „Pověřence pro ochranu osobních údajů“, kde Vám garantujeme zajištění komplexního servisu pro služby k GDPR včetně metodické podpory. Tato služba je standardně bez žádného paušálního poplatku.
- ✓ V případě, že by ve Vaší společnosti došlo k incidentu se ztrátou osobních dat a byli jste za tuto chybu vyšetřováni, nabízíme i spolupráci při řešení těchto situací. Nejsme však právníci tak, abychom Vás zastupovali u případného soudu. Věřím, že s naší pomocí se těmto událostem však vyhnete.

Ceník základních služeb GDPR	
GDPR – vnitropodniková směrnice	**od 1.900,- Kč**
Práce spojené s lokalizací směrnice na podmínky Vaší společnosti	**900,- Kč/hod**
Školení pracovníků	**1.200,- Kč/hod**
Cestovní výdaje při osobních návštěvách	**9,- Kč/Km + 450,- Kč/hod strávený čas na cestě**
Konzultace pověřence pro ochranu osobních dat pana Tomáše Urbana	**900,- Kč/hod**

Ceny jsou uvedeny bez DPH 21 %.

Certifikovaný pověřenec pro ochranu osobních dat:

TOMÁŠ URBAN

e-mail: tomas.urban@softbit.cz

tel.: 603 449 244

Nabídka služeb GDPR – pro naše zákazníky

V minulých letech jsme se všemi zákazníky v oblasti GDPR zpracovali základní pravidla pro ochranu a správu osobních údajů fyzických osob včetně školení odpovědných pracovníků v jednotlivých organizacích a společnostech.

Vzhledem k tomu, že téma ochrany osobních údajů fyzických osob se neustále vyvíjí, ani naše společná práce v této oblasti by neměla skončit. Jak víte, letos v dubnu naši zákonodárci konečně schválili Adaptační zákon číslo 110/2019 Sb., který upravuje část problematiky v ochraně osobních údajů podle nařízení GDPR. Připravili jsme proto pro Vás nabídku pro aktualizaci opatření pro ochranu osobních údajů právě ve Vaší společnosti či organizaci.

Nabídka obsahuje tyto služby:

Aktualizace směrnice

Nabízíme aktualizaci směrnice podle Českého adaptačního zákona a aktuálních výkladů nařízení GDPR. Aktualizovanou směrnici Vám předáme v tištěné i elektronické podobě.

Revize

Provedeme revizi všech činností spojených s ochranou a správou osobních dat. Zkontrolujeme opatření, která byla provedena v souvislosti se zavedením ochrany osobních údajů podle GDPR. O výsledku revize pro Vás sestavíme zprávu.

Ceník služeb GDPR	
Aktualizace směrnice GDPR pro rok 2020	od 1.900,- Kč včetně zaslání nové směrnice v tištěné podobě
Revize	900,- Kč/hod
Školení pracovníků	1.200,- Kč/hod
Konzultace pověřence pro ochranu osobních dat pana Tomáše Urbana	900,- Kč/hod

Ceny nezahrnují cestovní výdaje a jsou uvedeny bez DPH 21 %.

Školení pracovníků

Dále nabízíme individuální školení pro pracovníky organizace či společnosti v ochraně osobních údajů fyzických osob se zaměřením na aktuální stav legislativy a upozorníme na nejčastější chyby.

NA ZÁVĚR

Pevně věříme, že jste si našli čas na náš magazín GDPR a že námi poskytnuté informace, jsou pro Vás užitečné a praktické.

Za celý kolektiv pracovníků firmy Vám přeji hezký den a hodně sil do následujících měsíců.

Tomáš Urban
ředitel společnosti

Softbit Software, s.r.o.

Nad Dubinkou 1634

516 01 Rychnov nad Kněžnou

Tel.: 494 532 202, 494 534 354, fax: 494 377 63

e-mail: softbit@softbit.cz

www.softbit.cz

Tým společnosti Softbit Software s.r.o

Tomáš URBAN
(tel. 603 449 244)
- ✓ ředitel společnosti
- ✓ programátor účetnictví
- ✓ metodický konzultant informačních systémů

Simona URBANOVÁ
(tel. 736 753 733)
- ✓ ekonomka
- ✓ metodická konzultantka informačních systémů

Ing. Jeronym HOLÝ
(tel. 736 159 010)
- ✓ programátor majetek, výroba, jídelna
- ✓ metodický konzultant informačních systémů

Ing. Radim HOLÝ
(tel. 604 632 774)
- ✓ programátor sklady, prodej, odbyt
- ✓ metodický konzultant informačních systémů

Ing. Dana PEREMSKÁ
(tel. 736 753 735)
- ✓ administrativní pracovnice
- ✓ péče o zákazníky

David SMEJKAL
(tel. 603 365 779)
- ✓ hardware
- ✓ konzultant Vema HR, mzdy
- ✓ metodický konzultant informačních systémů

Bc. Tomáš HOLÝ
- ✓ programátor
- ✓ konzultant

Bc. Radek BERÁNEK
(tel. 736 753 734)
- ✓ všeobecný programátor
- ✓ konzultant Vema HR
- ✓ metodický konzultant informačních systémů

David URBAN
- ✓ všeobecný programátor