Vilímková Dudák &Partners

FORUM
Naše znalosti pro Váš úspěch

Zabezpečení osobních údajů

Mgr. Klára Valentová

12. 7. 2018

Nakladatelství FORUM s.r.o., divize školení a vzdělávání, Střelničná 1861/8a, Praha 8
tel: +420 251 550 576, fax: +420 251 512 422, office@forum-media.cz, www.forum-media.cz

Cíl webináře

- Seznámit účastníky s požadavky GDPR na zabezpečení osobních údajů
- Informovat o nejčastějších hrozbách a problémech v zabezpečení osobních údajů
- Dát příklady a návod na zabezpečení osobních údajů v organizaci

Osnova webináře

- Požadavky na zabezpečení osobních údajů podle zákona o ochraně osobních údajů a GDPR
- Bezpečnostní analýza (analýza rizik)
- Bezpečnostní opatření pro manuální a automatizované zpracování osobních údajů
- Bezpečnostní politika
- Evidence a hlášení bezpečnostních incidentů
- Školení o informační bezpečnosti
- Testování a aktualizace bezpečnostních opatření

Bezpečnost podle ZOOÚ

- Správce a zpracovatel jsou povinni přijmout taková opatření, aby nemohlo dojít **k neoprávněnému nebo nahodilému přístupu k osobním údajům, k jejich změně, zničení či ztrátě, neoprávněným přenosům, k jejich jinému neoprávněnému zpracování, jakož i k jinému zneužití osobních údajů**
- Tato povinnost platí i po ukončení zpracování osobních údajů

Bezpečnost podle ZOOÚ

- Správce nebo zpracovatel je povinen **zpracovat a dokumentovat přijatá a provedená technicko-organizační opatření** k zajištění ochrany osobních údajů v souladu se zákonem a jinými právními předpisy

Bezpečnost podle ZOOÚ

- V oblasti **automatizovaného zpracování** osobních údajů je správce nebo zpracovatel povinen:
  - zajistit, aby systémy pro automatizovaná zpracování osobních údajů používaly pouze oprávněné osoby
  - zajistit, aby fyzické osoby oprávněné k používání systémů pro automatizovaná zpracování osobních údajů měly přístup pouze k osobním údajům odpovídajícím oprávnění těchto osob, a to na základě zvláštních uživatelských oprávnění zřízených výlučně pro tyto osoby
  - pořizovat elektronické záznamy, které umožní určit a ověřit, kdy, kým a z jakého důvodu byly osobní údaje zaznamenány nebo jinak zpracovány
  - zabránit neoprávněnému přístupu k datovým nosičům

Bezpečnost podle ZOOÚ

- Zaměstnanci správce nebo zpracovatele a jiné osoby, které zpracovávají osobní údaje na základě smlouvy se správcem nebo zpracovatelem, mohou zpracovávat osobní údaje **pouze za podmínek a v rozsahu správcem nebo zpracovatelem stanoveném.**
- Povinnost zachovávat **mlčenlivost o osobních údajích a o bezpečnostních opatřeních**, jejichž zveřejnění by ohrozilo zabezpečení osobních údajů. Povinnost mlčenlivosti trvá i po skončení zaměstnání nebo příslušných prací.

Bezpečnost podle GDPR

- Správce a zpracovatel provedou vhodná technická a organizační opatření, aby zajistili **úroveň zabezpečení odpovídající danému riziku**, případně včetně:
  - pseudonymizace a šifrování osobních údajů
  - schopnosti zajistit neustálou důvěrnost, integritu, dostupnost a odolnost systémů a služeb zpracování
  - schopnosti obnovit dostupnost osobních údajů a přístup k nim včas v případě fyzických či technických incidentů
  - procesu pravidelného testování, posuzování a hodnocení účinnosti zavedených technických a organizačních opatření pro zajištění bezpečnosti zpracování

Bezpečnost podle GDPR

- **Přihlédnout** ke stavu techniky, nákladům na provedení, povaze, rozsahu, kontextu a účelům zpracování i k různě pravděpodobným a různě závažným rizikům pro práva a svobody fyzických osob
- **Zohlednit** zejména rizika, která představuje zpracování, zejména náhodné nebo protiprávní zničení, ztráta, pozměňování, neoprávněné zpřístupnění předávaných, uložených nebo jinak zpracovávaných osobních údajů, nebo neoprávněný přístup k nim

Bezpečnost podle GDPR

- Zajistit, aby jakákoliv **fyzická osoba**, která jedná z pověření správce nebo zpracovatele a má přístup k osobním údajům, **zpracovávala tyto osobní údaje pouze na pokyn správce**, pokud jí jejich zpracování již neukládá právní předpis EU nebo členského státu
- Možnost doložit soulad s požadavky na zabezpečení osobních údajů dodržováním schváleného **kodexu chování nebo získaného osvědčení**

Bezpečnostní analýza

- Posoudit dosavadní bezpečnostní opatření
- Provést analýzu rizik
- Případně zavést nová opatření
- Zpracovat a dokumentovat přijatá a provedená technicko-organizační opatření k zajištění ochrany osobních údajů (popis jednotlivých technických prostředků a postupů a organizačních pokynů pro osoby pracující s osobními údaji)

Hlavní příčiny úniku informací

- Hacking a malware (57%)
- Neúmyslné zveřejnění (22%)
- Přenosná zařízení a fyzická ztráta (17%)

Jak chránit svá data?

- Zastavit hlavní příčiny ztráty osobních údajů
- Zastavit hrozby přede dveřmi
- Zastavit lidské chyby

Bezpečnostní opatření

- Manuální (papírové) zpracování osobních údajů:
  - papírové složky musí být vždy uloženy v uzamykatelných skříňkách (odolnost skříněk proti vnějšímu útoku musí odpovídat rizikovosti zpracovávaných osobních údajů) a zásadně v prostorách společnosti (nikoli u zaměstnanců doma)
  - přístup ke skříňkám budou mít jen pracovníci, kteří papírové složky potřebují k výkonu práce
  - opatření proti hromadění dokumentů na tiskárnách nebo na pracovních stolech

Bezpečnostní opatření

- Automatizované (počítačové) zpracování osobních údajů:
  - softwarové a fyzické zabezpečení automatizovaných systémů (např. znemožnění tisku dat, připojení k síti jen uvnitř organizace)
  - omezení přístupových práv do jednotlivých systémů, aplikací, databází nebo sdílených disků
  - přístupy zabezpečit prostřednictvím bezpečných hesel (stanovení pravidel pro tvorbu hesla – počet a povaha znaků, pravidelné obměňování hesel)

Bezpečnostní opatření

- Automatizované (počítačové) zpracování osobních údajů:
  - omezení používání přenosných paměťových zařízení (USB), případně povinnost používat jen zaheslovaná zařízení
  - logování přístupu a operací s osobními údaji
  - šifrování disku (při používání mobilních zařízení – telefon, notebook) nebo souborů (např. při přenosu dat)
  - zákaz používat pro přenos osobních údajů prostý e-mail (např. použít datovou schránku, zasílat pseudonymizovaná data – identifikační údaje jsou nahrazeny kódem nebo číslem, zasílat zašifrované soubory)

Bezpečnostní opatření

- Zabezpečení objektu, přístupových cest a prostor (např. poplachové systémy, kamerové systémy, bezpečnostní služba apod.)
- Pravidelné testování, posuzování a hodnocení zavedených opatření, včetně vyvození důsledků pro zaměstnance
- Smlouvy o zpracování osobních údajů s dodavateli (zpracovateli) – primární odpovědnost za zpracování vždy na správci

Bezpečnostní opatření

- Stanovit přiměřené lhůty pro uchovávání osobních údajů:
  - u klientů – rozlišovat aktivní/neaktivní klienty – max. 10 let u neaktivních klientů
  - přímý marketing – doba neurčitá (do vznesení námitky)
  - v osobních spisech zaměstnanců (10 - 20 let) – po skončení pracovního poměru provést revizi osobního spisu a zlikvidovat nepotřebné dokumenty (např. životopisy, kopie diplomů, fotografie); mzdové účely (mzdový list – 30 let)
  - pro účely ochrany práv správce (např. tříletá promlčecí lhůta v případě potenciálního soudního sporu)

Bezpečnostní opatření

- Zavést systém pro pravidelnou likvidaci osobních údajů, u nichž uplynula lhůta k uchování:
  - např. automatizované sjetiny se seznamem osob, jejichž údaje mají být zlikvidovány (výmaz nebo anonymizace)
  - pravidelná skartace dokumentů podle skartačního řádu

Bezpečnostní politika

- Zahrnuje dvě úrovně požadavků – MUST (musí)/SHOULD (doporučeno)
- Hodnocení jednotlivých bodů politiky podle skutečné praxe v organizaci
- Definuje obecné požadavky, principy a cíle vedoucí k dosažení bezpečnosti informací, které organizace zpracovává nebo jsou jí a jejím zaměstnancům dostupné
- Komplexní a systematický přístup k řešení bezpečnosti informací - Information Security Management System

Bezpečnostní incidenty

- Připravit postup při výskytu bezpečnostních incidentů (tj. jakékoli porušení zabezpečení osobních údajů – např. zaslání osobních údajů nesprávnému adresátovi, dočasná nebo úplná ztráta složky studenta, hackerské útoky, porušení povinnosti mlčenlivosti zaměstnancem):
  - bezpečnostní incidenty musejí být detekovány (zjištěny) – možnost využít speciální softwarové vybavení, povinnost hlášení bezpečnostních incidentů určené osobě
  - bezpečnostní incidenty musejí být evidovány
  - bezpečnostní incidenty musejí být vyhodnoceny s ohledem na rizika pro subjekty údajů

Bezpečnostní incidenty

- bezpečnostní incidenty s pravděpodobným rizikem pro subjekty údajů musejí být ohlášeny Úřadu pro ochranu osobních údajů do 72 hodin po zjištění bezpečnostního incidentu (standardně téměř všechny incidenty, pokud není incident okamžitě zjištěn a jakékoli negativní dopady eliminovány)
- bezpečnostní incidenty s vysokým rizikem pro subjekty údajů musejí oznámeny přímo subjektům údajů (např. ztráta osobní složky zaměstnance)
- bezpečnostní incidenty musejí být vyřešeny a musejí být přijata opatření ke zmírnění možných nepříznivých dopadů a preventivní opatření do budoucna
- zpracovatelé musejí neprodleně hlásit bezpečnostní incidenty správci

Školení pracovníků

- Proškolit všechny osoby, které zpracovávají osobní údaje nebo k nim mají přístup:
  - zdroj pro školení – webinář, on-line školení, in-house školení, externí školení
  - poučit o povinnosti mlčenlivosti
  - případně uvést konkrétní pokyny ke zpracování a ochraně osobních údajů do pracovních smluv, popisu pracovní pozice nebo vnitřní bezpečnostní směrnice

Testování a aktualizace opatření

- Pravidelné bezpečnostní audity
- Penetrační testy
- Testování zaměstnanců
- Pravidelná aktualizace IT systémů
- Sledování trendů v zabezpečení dat (posouzení novinek ve vztahu k ochraně soukromí zaměstnanců – zařízení splňující princip „privacy by design“)

Závěrečné shrnutí

- Udělat si pořádek v systémech a datech
- Stanovit odpovědnost za bezpečnost zpracování osobních údajů
- Vyhodnotit rizika a současný stav zabezpečení
- Zavést a zdokumentovat jednotlivá bezpečnostní opatření
- Vytvořit bezpečnostní politiku
- Vytvořit systém evidence a hlášení bezpečnostních incidentů
- Pravidelně školit a testovat zaměstnance
- Pravidelně testovat a aktualizovat IT systémy a jejich zabezpečení

Dotazy?

Mgr. Klára Valentová, advokát

Vilímková Dudák & Partners, advokátní kancelář, s.r.o.

Karolinská 661/4, 186 00 Praha 8
Tel.: +(420) 222 814 911

Fax: +(420) 222 814 915
klara.valentova@vilimkovadudak.cz

www.vilimkovadudak.cz

Vilímková Dudák &Partners

FORUM
Naše znalosti pro Váš úspěch

Děkuji za pozornost!

Tento webinář pořádá

Nakladatelství FORUM s.r.o., divize školení a vzdělávání
Střelničná 1861/8a, Praha 8
tel: +420 251 115 576
fax: +420 251 512 422
office@forum-media.cz
www.forum-media.cz
www.forum-media.sk