Severozápad

EVROPSKÁ UNIE

Regionální rada regionu soudržnosti Severozápad

ZPRÁVA O ČINNOSTI POVĚŘENCE PRO OCHRANU OSOBNÍCH ÚDAJŮ ZA ROK 2019

Verze 1

25. 2. 2020

1. identifikační údaje správce údajů

název:	Regionální rada regionu soudržnosti Severozápad – Úřad Regionální rady regionu soudržnosti Severozápad
sídlo:	Ústí nad Labem, Berní 2261/1
právní forma:	právnická osoba zřízená zákonem č. 248/2000 Sb., o podpoře regionálního rozvoje, v platném znění
zastoupený:	Bc. Janou Havlicovou, MBA, ředitelkou Úřadu Regionální rady regionu soudržnosti Severozápad
identifikační číslo:	75082136
pověřenec pro ochranu osobních údajů:	Mgr. Edit Cermanová
kontaktní údaje:	736 650 711/edit.cermanova@nuts2severozapad.cz

2. obecné úkoly pověřence pro ochranu osobních údajů

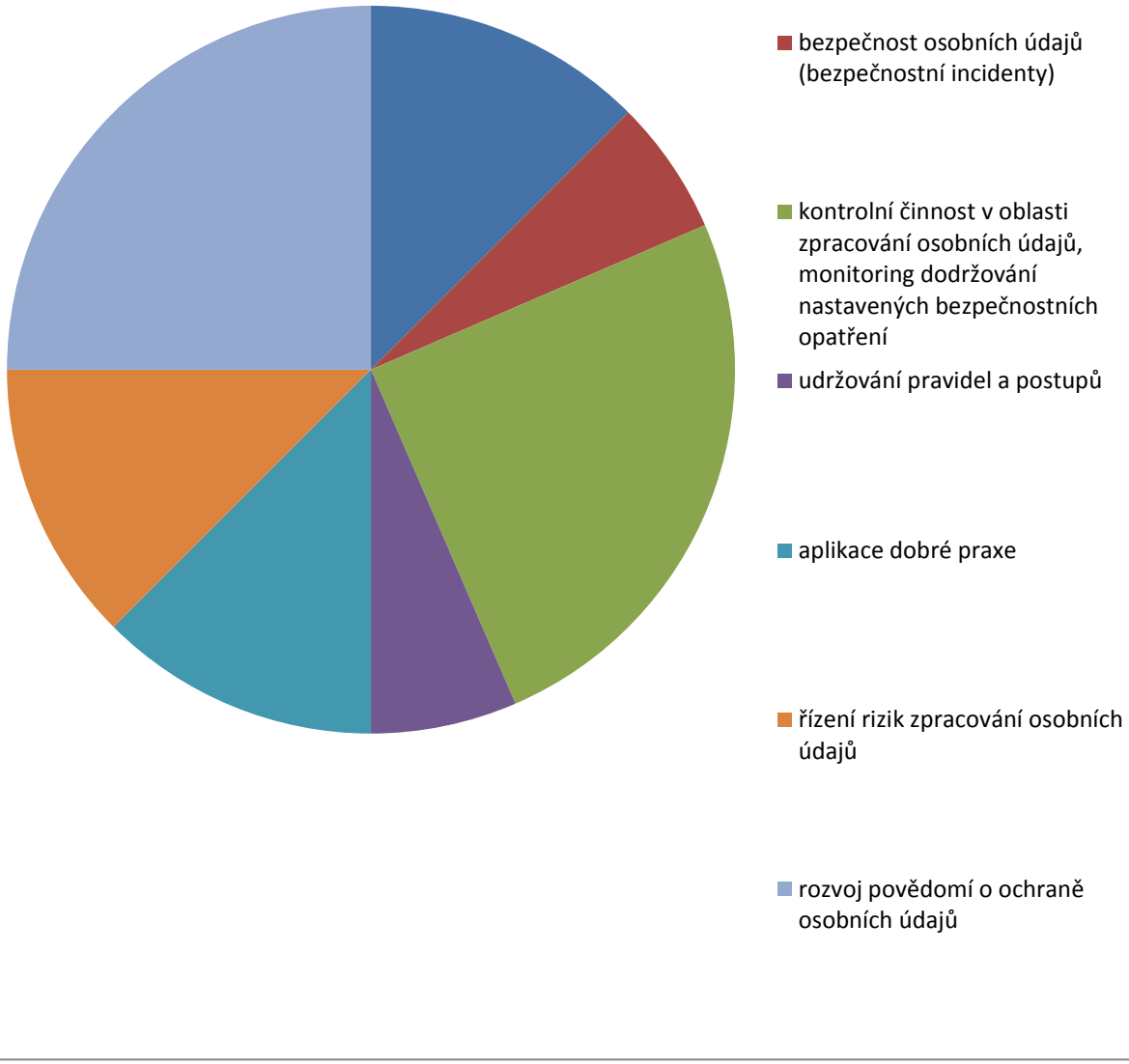
Pověřenec pro ochranu osobních údajů (dále jen „DPO“, z angl. Data Protection Officer) vykonává nezávislou, objektivně ujišťovací a konzultační činnost s cílem zvyšovat v rámci Regionální rady regionu soudržnosti Severozápad (dále jen „správce údajů“ nebo „RR SZ“) povědomí o problematice ochrany osobních údajů a zajistit vždy co nejvyšší možný standard zpracování a ochrany osobních údajů.

Obecnými úkoly DPO jsou:

- poskytování informací a poradenství zaměstnancům RR SZ a členům orgánů RR SZ, kteří provádějí zpracování osobních údajů o jejich povinnostech podle GDPR a dalších předpisů Evropské unie nebo České republiky v oblasti ochrany údajů,
- působení jako kontaktní místo pro subjekty údajů ve všech záležitostech souvisejících se zpracováním jejich osobních údajů a s výkonem jejich práv podle GDPR,
- monitorování souladu prostředí RR SZ s GDPR, dalšími předpisy Evropské unie nebo České republiky v oblasti ochrany osobních údajů, včetně rozdělení odpovědnosti, zvyšování povědomí a odborné přípravy pracovníků zapojených do operací zpracování a souvisejících auditů,
- poskytování poradenství na požádání, pokud jde o posouzení vlivu na ochranu osobních údajů a monitorování jeho uplatňování podle článku 35 GDPR,
- spolupráce s dozorovým úřadem, působení jako kontaktní místo pro dozorový úřad v záležitostech týkajících se zpracování, včetně předchozí konzultace podle článku 36 GDPR, a případně řízení konzultací v jakékoli jiné věci,
- řízení záznamů o zpracování osobních údajů podle čl. 30 GDPR.

DPO bere při plnění svých úkolů patřičný ohled na riziko spojené s operacemi zpracování a současně přihlíží k povaze, rozsahu, kontextu a účelům zpracování.

3. rozsah činností pověřence pro ochranu osobních údajů v roce 2019



4. konkrétní činnosti DPO v roce 2019 – plán

činnost	četnost	způsob
zajištění souladu s právními předpisy	průběžně	- monitorovaní legislativních změn, doporučení a nálezů Úřadu pro ochranu osobních údajů a pracovní skupiny WP29 - aktualizace vnitřních předpisů správce údajů
řízení bezpečnosti osobních údajů (bezpečnostní incidenty)	dle výskytu 1x ročně do 31. 12. 2019	- ve spolupráci se zaměstnanci, IT techniky a jinými pověřenci pro ochranu osobních údajů - návrh rychlého řešení, návrh opatření proti opakování bezpečnostního incidentu - ve spolupráci s IT techniky provedení hackerského útoku na systémy správce údajů, následné kroky po vyhodnocení chování zaměstnanců
kontrolní činnost v oblasti zpracování osobních údajů, monitoring dodržování nastavených bezpečnostních opatření	2x ročně, do 30. 6. 2019, do 31. 12. 2019	- kontrola dodržování pravidel IT bezpečnosti [kontrola hesel (lepíky na monitoru, hesla zapsaná v kalendáři), kontrola obsahu sdílených disků] - kontrola dodržování pravidel fyzické bezpečnosti (uzamykání kanceláří) - kontrola docházkového systému (oprávněný náhled)
udržování pravidel a postupů	dle výskytu nesouladu	- aktualizace vnitřních předpisů správce údajů, návrh změny fyzického prostředí správce údajů
aplikace dobré praxe	po ukončení dalších činností, průběžně dle potřeby 1x ročně, k 31. 12. 2019	- poskytování výkladových stanovisek a doporučení pro správce údajů - vyhodnocení funkčnosti a efektivnosti opatření pro zpracování osobních údajů a jejich ochranu
řízení rizik zpracování osobních údajů	alespoň 1x ročně, k 31. 12. 2019	- aktualizace Analýzy rizik zpracování osobních údajů - kontrola souladu Záznamu o zpracování osobních údajů s praxí
rozvoj povědomí o ochraně osobních údajů	průběžně 1x ročně, do 30. 6. 2019	- poskytování výkladových stanovisek a doporučení pro zaměstnance správce údajů - školení pro zaměstnance správce údajů

4.1. soulad s právními předpisy

V roce 2019 byly aktualizovány tyto předpisy RR SZ (výčet předpisů je omezen na změny související s ochranou osobních údajů):

- Dodatek č. 3 k Řádu č. R-3/2018 Pracovní řád,
- Řád č. R-1/2019 Organizační řád + Dodatek č. 1,
- Dodatky č. 2 a 3 ke Směrnici č. S-7/2018 na ochranu osobních údajů,
- Dodatek č. 1 ke Směrnici č. S-10/2018 o ICT,
- Dodatek č. 1 ke Směrnici č. S-12/2018 o zajištění BOZP,
- Směrnice č. S-3/2019 o zadávání veřejných zakázek,
- Směrnice č. S-4/2019 o přijímání, evidování a vyřizování stížností.

4.2. bezpečnost osobních údajů (bezpečnostní incidenty)

V roce 2019 nebyly řešeny žádné bezpečnostní incidenty.

Zamýšlený hackerský útok na systémy správce údajů nebyl proveden, a to z finančních důvodů. Chování zaměstnanců při útoku bylo prověřeno teoreticky 11. listopadu 2019 v rámci školení „Interní akty řízení“, kterého se zúčastnili všichni zaměstnanci RR SZ.

4.3. kontrolní činnost v oblasti zpracování osobních údajů, monitoring dodržování nastavených bezpečnostních opatření

V období 28. 2. 2019 – 30. 11. 2019 probíhal u správce údajů interní audit „Audit implementace GDPR“. Interní audit konstatoval, že prověřovaná pravidla a zásady na ochranu osobních údajů zavedená do procesů vnitřního kontrolního systému RR SZ včetně přiřazených odpovědností, jsou v souladu s požadavky GDPR a správce osobních údajů uplatňuje vhodnou koncepci pro ochranu osobních údajů.

9. červenec 2019 byl stanoven jako nejzazší datum pro vyčištění sdílených disků. Všichni zaměstnanci byli poučeni o důvodech vedoucích k tomuto kroku a byl jim navržen nejlepší způsob. Zaměstnanci podle zájmu obdrželi externí disky a na sdílených discích byly zřízeny nové složky s předem definovanými přístupy k nim.

4.4. udržování pravidel a postupů

Z kontrolních činností nevyplynul žádný nesoulad, žádné návrhy na změnu vnitřních předpisů či návrhy na změny fyzické bezpečnosti nebyly vzneseny.

4.5. aplikace dobré praxe

DPO průběžně konzultuje dotazy zaměstnanců správce údajů a členů orgánů RR SZ. Nejzávažnější konzultace, která proběhla v roce 2019, se týkala nového systému tzv. e-Neschopenek.

Funkčnost a efektivnost opatření pro zpracování osobních údajů a jejich ochranu byla vyhodnocena ve spolupráci s Interním auditem v rámci interního auditu „Audit implementace GDPR“.

4.6. řízení rizik zpracování osobních údajů

V roce 2019 byla celkem 2x aktualizována Analýza rizik zpracování osobních údajů. Bylo doplněno:

- právní a ostatní předpisy, na základě kterých probíhá zpracování osobních údajů,
- agenda, ve které dochází ke zpracování osobních údajů,
- agenda přístupu k osobním údajům,
- příjemci osobních údajů.

V roce 2019 bylo vypracováno 40 nových Záznamů o činnostech zpracování, z nichž jeden byl následně aktualizován.

4.7. rozvoj povědomí o ochraně osobních údajů

Dne 11. listopadu 2019 proběhlo školení pro všechny zaměstnance RR SZ zaměřené mj. na zásady ochrany osobních údajů. Z důvodu probíhajících legislativních změn, kdy by nebylo možné zaručit, že předkládané údaje budou nadále platné, školení proběhlo až ve 2. pololetí.

5. další činnosti DPO v roce 2019

5.1. pracovní skupiny regionálních rad

14. 5. 2019 – PS VPL

13. 11. 2019 – PS LAN

Zástupci regionálních rad, kteří budou vykonávat funkci pověřenců, vytipovali dokumentaci, která se regionálních rad týká, a slíbili si budoucí spolupráci při její tvorbě a aktualizaci.

5.2. absolvovaná školení

30. 1. 2019 – GDPR v české praxi: Adaptační zákon a změny v ochraně osobních údajů

3. 10. 2019 – Penetrační testy a analýza rizik

25. 10. 2019 – zákon o kybernetické bezpečnosti

5.3. další činnosti

nastavení pravidel k agendě e-Neschopenek

zpracování formuláře „mlčenlivosti“ nad rámec běžného pracovního výkonu pro pracovnice podatelny

5.4. nápravná opatření přijatá ke zjištěním z interního auditu

Zjištění: prakticky realizované zálohování dat nekoresponduje s Přílohou č. 1 Zálohovací plán Směrnice S-10/2018 o ICT.

Opatření: aktualizovat Přílohu č. 1 Zálohovací plán, termín 31. 12. 2019.

Plnění: splněno.

Zjištění: nejsou nastaveny postupy pro ohlášení bezpečnostního incidentu.

Opatření: nastavit postupy a určit odpovědnosti, termín 28. 2. 2020.

Plnění: bude podána žádost o prodloužení termínu – Směrnice č. S-7/2008 na ochranu osobních údajů podléhá novelizaci v souvislosti se změnou organizační struktury RR SZ, novelizace bude účinná k 1. 4. 2020. Vypracovat dodatek k 28. 2. 2020 a následně novelizovat celou směrnici by bylo neefektivní.

Zjištění: Nejsou definovány postupy a odpovědnosti pro urychlené a efektivní řešení bezpečnostního incidentu.

Opatření: uzavřít dodatek ke smlouvě o zajištění ICT a aktualizovat povinnosti DPO, termín 28. 2. 2020.

Plnění: dodatek ke smlouvě o zajištění ICT bude uzavřen v termínu, k dodatku směrnice č. S-10/2018 o ICT viz výše.

Zjištění: nejsou řešeny případy porušení zabezpečení osobních údajů s vysokým rizikem pro práva a svobody fyzických osob.

Opatření: stanovit kompetence a postupy pro oznamování těchto případů, termín 28. 2. 2020.

Plnění: viz výše.

Zjištění: DPO neinformoval Výbor Regionální rady regionu soudržnosti Severozápad (dále jen „VRR“) o své činnosti a nevypracoval zprávu o činnosti DPO za rok 2018.

Opatření: vypracovat a předložit VRR zprávu o činnosti DPO za rok 2019 obsahující i informace z předchozích let, v termínu dle konání VRR v roce 2020.

Plnění: splněno.

Zjištění: DPO nepředložil VRR plán práce DPO pro rok 2019.

Opatření: předložit plán práce DPO pro rok 2020, v termínu dle konání VRR v roce 2020.

Plnění: splněno.

6. činnosti DPO v předchozím období

2017:

Proběhlo Asistované zhodnocení bezpečnostních opatření pro zajištění ochrany a bezpečnosti osobních údajů, ze kterého vyplynula tato rizika:

- bezpečné předávání a výměna informací,
- řízení dodavatelů v oblasti dodavatelsko-odběratelských vztahů,
- sloučení rolí, které jsou odpovědné za provoz a bezpečnost (externí správce ICT),
- bezpečné používání mobilních zařízení,
- kontroly a auditu v oblasti bezpečnosti ICT,
- budování bezpečnostního povědomí u zaměstnanců v oblasti ochrany a nakládání s osobními údaji.

DPO (v období jen uvažovaný) se zúčastnil těchto školicích akcí:

- 23. 2. 2017 Ochrana osobních údajů a GDPR – nové nařízení EU,
- 20. 11. 2017 GDPR pro veřejný sektor.

2018:

Byla aplikována doporučení z výše uvedené analýzy, konkr.:

- aktualizovány vnitřní předpisy RRSZ:
  - Řád č. R-3/2018 Pracovní řád;
  - Řád č. R-1/2018 Organizační řád;
  - Dodatky č. 3 a 4 ke Směrnici č. S-4/2014 o etickém chování zaměstnanců;
  - Směrnice č. S-7/2018 na ochranu osobních údajů + Dodatek č. 1;
  - Směrnice č. S-10/2018 o ICT;
  - Směrnice č. S-12/2018 o zajištění BOZP;
  - Směrnice č. S-13/2018 o kontrolách a auditech a vypořádávání jejich závěrů,
- nastavena přísnější pravidla související s ITC bezpečností: zpracováno bezpečnostní desatero, zpřísněny podmínky pro tvorbu a opakování hesel, nastavení přístupových práv na sdílené disky, nastaveny podmínky pro předávání osobních údajů,
- 6. 6. 2018 a 25. 7. 2018 proběhla školení pro všechny zaměstnance RR SZ.

Dále byla pracována dokumentace související s ochranou osobních údajů (instruktáž/souhlas se zpracováním), výchozí Analýza rizik zpracování osobních údajů, následně 2x aktualizována, zpracovány a podepsány dodatky (celkem 13) k dodavatelským smlouvám s dodavateli, kteří se setkávají s osobními údaji nebo se s nimi setkávat mohou, byl řešen jeden bezpečnostní incident.

10. 5. 2018 byl Úřadu pro ochranu osobních údajů oznámen DPO, informace zveřejněna na internetových stránkách a úřední desce RR SZ.

DPO se 7. 3. 2018 a 4. 12. 2018 účastnil PS VPL a 5. 3. 2018 absolvoval školení „Ochrana osobních údajů a archivace dat ve mzdové a personální agendě“ a 15. 11. 2018 školení „Audit činnosti pověřence v rámci sytému zpracování osobních údajů“.

7. podpisová doložka

Vypracovala: Cermanová, pověřená k výkonu funkce Pověřence pro ochranu osobních údajů, dne 25. 2. 2020.

… … …

Zprávu o činnosti DPO za rok 2019 předložil DPO vedoucím organizačních útvarů RR SZ a členům PS PRD k připomínkám dne 25. 2. 2020. Připomínky vedoucích organizačních útvarů RR SZ a členů PS PRD byly projednány a vypořádány.

Zpráva o činnosti Pověřence pro ochranu osobních údajů za rok 2019 byla schválena Výborem Regionální rady regionu soudržnosti Severozápad usnesením č. 9/127/2020 ze dne 23. 3. 2020.

Berní 2261/1
400 01 Ústí nad Labem
tel.: 475 240 600
e-mail: ridiciorgan@nuts2severozapad.cz

Severozápad

EVROPSKÁ UNIE

Regionální operační program regionu soudržnosti Severozápad
Podporováno z Evropského fondu pro regionální rozvoj
„Vize přestane být snem"