Úřad pro ochranu
osobních údajů

Ohlášení porušení zabezpečení osobních údajů dle GDPR

☐ prvotní ohlášení ☐ doplnění ohlášení

1. Správce, u něhož došlo k porušení zabezpečení

název nebo jméno a příjmení

sídlo nebo bydliště – ulice, město, PSČ, stát

IČO

2. Pověřenec správce *(byl-li jmenován)* **nebo jiná kontaktní osoba**

jméno a příjmení

telefon

e-mail

doručovací adresa

3. Další subjekt zapojený do dotčeného zpracování *(zpracovatel, další správce, příjemce)*

role *(zpracovatel–správce–příjemce)*

název nebo jméno a příjmení

sídlo nebo bydliště – ulice, město, PSČ, stát

IČO

4. Průběh incidentu *(pokud je znám)*[1]

datum a čas vzniku porušení

datum a čas ukončení porušení

datum a čas zjištění porušení správcem

Pokud je oznamován více než 72 hodin po jeho zjištění, uveďte důvody tohoto zpoždění.

1 Pokud nejsou známy přesné datum a čas zjištění porušení (čas vzniku a doba trvání), uveďte co možná nejpřesnější údaje, které jsou správci známy.

5. Popis vzniku porušení *(příčiny porušení)*

Jak k porušení došlo, uveďte pravděpodobnou příčinu

- externí útok *(upřesněte níže)*
- interní útok *(upřesněte níže)*
- selhání systému
- nedbalost
- jiná příčina

Podrobnější popis příčiny porušení:

6. Popis zjištěných účinků *(označte zjištěné účinky porušení)*

- porušení důvěrnosti dat (v případě neoprávněného nebo náhodného poskytnutí nebo zpřístupnění osobních údajů)
- porušení integrity dat (v případě neoprávněného nebo náhodného pozměnění osobních údajů)
- porušení dostupnosti dat (v případě náhodné nebo neoprávněné ztráty, přístupu nebo zničení osobních údajů např. protiprávní zašifrování)
- jiné (upřesněte)

7. Kategorie dotčených osobních údajů *(označte kategorie dotčených údajů)*

- identifikační údaje (jméno, příjmení, datum narození, rodné číslo, jiný identifikátor)
- kontaktní údaje (např. adresa, e-mail, telefon)
- ekonomické a finanční údaje
- data o poloze (lokační údaje)
- údaje o trestním odsouzení, o spáchání přestupku
- jiné (upřesněte)

upřesněte

7.1. zvláštní kategorie údajů

- údaje vypovídající o rasovém nebo etnickém původu
- údaje vypovídající o politických názorech a členství v odborech
- údaje vypovídající o filozofickém přesvědčení nebo náboženském vyznání
- údaje o zdravotním stavu
- údaje o sexuálním životě nebo orientaci
- genetické a biometrické údaje, jsou-li zpracovány za účelem jednoznačné identifikace fyzické osoby

upřesněte

8. Kategorie subjektů údajů *(označte kategorie fyzických osob dotčených porušením)*

- zaměstnanci nebo osoby v pracovněprávním vztahu ke správci/zpracovateli
- uživatelé
- zákazníci (bývalí, současní i budoucí)
- pacienti
- zranitelné osoby (např. děti)
- jiné (upřesněte)

8.1. přibližný počet dotčených subjektů údajů

8.2. přibližný počet dotčených záznamů osobních údajů

9. Důsledky – povaha pravděpodobného dopadu na ohrožené subjekty údajů

(Označte pravděpodobné fyzické, materiální nebo nemateriální škody nebo významné důsledky na dotčené subjekty údajů a specifikujte míru pravděpodobnosti a závažnosti důsledků pro subjekty údajů)

- ztráta kontroly nad osobními údaji
- data mohou být spojena s dalšími informacemi
- data mohou být využita k jiným/nekalým účelům
- data mohou být změněna a následně použita k jiným účelům
- neoprávněné obrácení pseudonymizace (zpracovávaná data již mohou být přiřazena k identifikované nebo identifikovatelné fyzické osobě)
- ztráta nebo změna schopnosti správce /zpracovatele poskytovat služby pro dotčené subjekty údajů
- krádež identity
- podvod
- omezení práv dotčených subjektů údajů
- diskriminace dotčených subjektů údajů
- finanční ztráty
- poškození pověsti
- ztráta důvěrnosti dat chráněných profesním tajemstvím
- ostatní *(upřesněte)*

10. Opatření přijatá PŘED vznikem porušení zabezpečení

10.1. označte a popište relevantní dokumenty, kterými je správcem řízeno zpracování osobních údajů

- vnitřní předpisy
- písemné pokyny zaměstnancům
- závazné politiky správy a zabezpečení dat a informací
- smlouva o zpracování osobních údajů
- jiné *upřesněte*

10.2. další organizační a technická opatření, režimová opatření přijatá před porušením *(např. fyzické, organizační a režimové zabezpečení – uzamykatelné skříně, místnosti, řízení přístupů, hesla, logování)*

10.3. uveďte, jakými prostředky (HW i SW) byly ohrožené osobních údaje zpracovávány

10.4. jiné bezpečnostní nástroje *(např. šifrování)*

11. Opatření zvolená k řešení/nápravě porušení zabezpečení

11.1. Popište a doložte opatření, přijatá k řešení/porušení zabezpečení *(popište, v čem opatření spočívala, např. zablokování uživatelských účtů, podání trestního oznámení, hlášení kybernetického bezpečnostního incidentu, apod.)*

Případně přijatá opatření doložte jako přílohu formuláře

11.2. datum a čas přijatých opatření

11.3. oznámení dotčeným fyzickým osobám

a) **ano** *(doplňte datum, kdy a jakým způsobem, počet informovaných subjektů údajů + doložte obsah oznámení v příloze formuláře)*

- Jestliže byl dotčeným osobám zaslán návod či doporučení, jak se mají zachovat, popište jej + doložte obsah v příloze formuláře

b) **ne, ale budou** informovány (doplňte předpokládané datum, kdy a jakým způsobem + následně informaci doplňte)

c) **ne, nebudou** informovány (odůvodněte tento postup – vyberte z následujících možností a tuto možnost odůvodněte)

- porušení zabezpečení pravděpodobně nepředstavuje vysoké riziko pro práva a svobody dotčených fyzických osob
- s ohledem na přijatá technická a organizační opatření, dotčené osobní údaje jsou nesrozumitelné pro všechny neoprávněné osoby (např. šifrování)
- správce přijal následná opatření, která zajistí, že vysoké riziko pro práva a svobody dotčených fyzických osob již nebude pravděpodobně naplněno
- představovalo by nepřiměřené úsilí informovat každou fyzickou osobu individuálně (+ uveďte způsob účiněného veřejného oznámení)

(upřesněte odůvodnění)

d) **zatím nebylo rozhodnuto** o informování dotčených osob (upřesněte důvod)

11.4. komunikace s dalšími orgány (uveďte, zda jste dané porušení zabezpečení ohlásili dalším orgánům, např. policie, jiný úřad, zahraniční dozorový úřad)

- **ne**
- **ano**

a. uveďte **název orgánu**, **č.j.,** je-li známo, **event. informaci o šetření**

12. přeshraniční zpracování

12.1 Je zpracování, které bylo porušením dotčeno, přeshraničním zpracováním ve smyslu čl. 4 bodu 23 obecného nařízení?

- ne
- ano

a. uveďte, **ve kterých členských státech EU[2] má správce provozovny**, v souvislosti s jejichž činností probíhá dané zpracování, označte též jeho hlavní provozovnu v EU *(ve smyslu čl. 4 bodu 16 obecného nařízení, tedy ústřední správu nebo provozovnu, ve které jsou činěna rozhodnutí o účelech a prostředcích zpracování a která má současně pravomoc tato rozhodnutí vymáhat)*

b. jsou nebo pravděpodobně budou daným zpracováním podstatně dotčeny ***subjekty údajů ve více členských státech EU****? Jestliže ano, identifikujte jedinou provozovnu a uveďte důvod podstatného dotčení subjektů údajů a výčet členských států, v nichž mají dotčené subjekty údajů bydliště.*

12.2 Ohlášení je činěno vůči Úřadu jako

- **vedoucímu dozorovému úřadu**
- **dotčenému dozorovému úřadu** *(v tomto případě označte vedoucí dozorový úřad a doplňte informaci o oznámení tomuto úřadu)*

odůvodněte:

2 Pro účely tohoto formuláře jsou pod pojmem „členské státy EU" zahrnuty také státy Evropského hospodářského prostoru, a to Island, Norsko a Lichtenštejnsko.

12.3 V jakých členských státech EU mají bydliště subjekty údajů, které jsou dotčeny předmětným porušením zabezpečení?

13. subjekt, který není usazen v EU

13.1 V případě, že správce, případně zpracovatel, není usazen v žádném členském státě EU, uveďte informace o jeho zástupci v EU *(kontaktní údaje zástupce, informace o jeho jmenování)*

14. další informace o případu porušení zabezpečení *(zejména dodatečné informace důležité pro vyhodnocení daného případu, případně informace pro doplnění ohlášení)*