

Template pro oznámení porušení zabezpečení osobních údajů

Formulář slouží jako inspirace, jak může být provedeno oznámení porušení bezpečnosti osobních údajů. Je možné jej upravit dle specifických požadavků Dozorového úřadu a dané společnosti.

Připraveno s využitím zahraničních zdrojů – tým [GDPR24.EU](https://gdpr24.eu)

I. Identifikační údaje Správce

Tato informace je pro využití Dozorovým úřadem, nikoliv ke sdílení se třetími stranami

1. Identifikační údaje společnosti

Název společnosti:

Adresa:

PSČ:

Město:

Stát:

2. Pověřenec pro ochranu osobních údajů nebo kontaktní osoba pro získání dalších informací.

Jméno:

Pozice:

PSČ:

Město:

Adresa:

Stát:

E-mail:

Telefon:

3. Typ OZNÁMENÍ

Úplné oznámení (pole zahrnutá v sekci II a III by měla být vyplněna do 72 hodin od zjištění porušení zabezpečení)

Oznámení ve dvou krocích (pole zahrnutá v sekci II by měla být vyplněna do 72 hodin od zjištění a pole zahrnutá v sekci III by měla být vyplněna postupně bez dalšího zbytečného odkladu.)

II. Hlavní údaje k porušení zabezpečení

K vyplnění a sdílení s Dozorovým úřadem v rámci prvních 72 hodin od zjištění

1. Odvětví dotčené strany včetně kódu CZ-NACE (viz NACE.CZ)

- | | |
|---|--|
| <input type="checkbox"/> A/ Zemědělství, lesnictví, rybářství | <input type="checkbox"/> L/ Činnosti v oblasti nemovitostí |
| <input type="checkbox"/> B/ Těžba a dobývání | <input type="checkbox"/> M/ Profesní, vědecké a technické činnosti |
| <input type="checkbox"/> C/ Zpracovatelský průmysl | <input type="checkbox"/> N/ Administrativní a podpůrné činnosti |
| <input type="checkbox"/> D/ Energetika, plynárenství, teplárenství | <input type="checkbox"/> O/ Veřejná správa, policie a obrana |
| <input type="checkbox"/> E/ Zásobování vodou, kanalizace | <input type="checkbox"/> P/ Sociální správa, úřady práce |
| <input type="checkbox"/> F/ Stavebnictví | <input type="checkbox"/> P/ Vzdělávání |
| <input type="checkbox"/> G/ Velkoobchod a maloobchod | <input type="checkbox"/> Q/ Zdravotní a sociální péče |
| <input type="checkbox"/> H/ Doprava, autoopravárenství a skladování | <input type="checkbox"/> R/ Kulturní, zábavní a rekreační činnosti |
| <input type="checkbox"/> I/ Ubytování, stravování a pohostinství | <input type="checkbox"/> S/ Činnosti domácností |
| <input type="checkbox"/> J/ Informační a komunikační činnosti | <input type="checkbox"/> T/ Činnosti exiteritoriálních organizací a orgánů |
| <input type="checkbox"/> K/ Peněžnictví a pojišťovnictví | <input type="checkbox"/> S/ Ostatní činnosti (prosím upřesněte): |

2/ Počet zaměstnanců

- | | |
|---------------------------------|-----------------------------------|
| <input type="checkbox"/> 1-9 | <input type="checkbox"/> 250-749 |
| <input type="checkbox"/> 10-49 | <input type="checkbox"/> 750-1000 |
| <input type="checkbox"/> 50-249 | <input type="checkbox"/> > 1000 |

3. Velikost organizace — obrat

- | | |
|--|--|
| <input type="checkbox"/> ≤ € 50 mil. Kč | <input type="checkbox"/> ≤ € 1 mld. Kč |
| <input type="checkbox"/> ≤ € 250 mil. Kč | <input type="checkbox"/> > € 1 mld. Kč |

4. Členský stát, kde má společnost hlavní provozovnu

5. Členský stát, kde došlo k porušení zabezpečení

6. Datum a čas porušení zabezpečení (ve formátu DD. MM. RRRR HH.MM):

7. Datum a čas zjištění zabezpečení (ve formátu DD. MM. RRRR HH.MM):

8. Znáte příčinu porušení zabezpečení?

Škodlivý útok (Doplňte, zda se jedná o útok interní nebo externí)

Interní

Externí

Nehoda (selhání systému)

Nedbalost (lidské pochybení)

Jiná (prosím upřesněte):

9. Pokud se jednalo o škodlivý útok, co bylo příčinou porušení zabezpečení?

Trojský kůň

Malware

Zašifrování (Ransomware)

CEO-fraud

Phishing

Vydírání

Distributed Denial of Service (DDoS, DoS)

Jiné (prosím upřesněte):

10. Jaký je pravděpodobný dopad porušení zabezpečení?

Zveřejnění osobních údajů

Přímá finanční újma

Krádež osobních údajů

Přerušování provozu

Krádež identity nebo fraud

Odpovědnosti za škody třetích stran

Ztráta dostupnosti osobních údajů

Poškození reputace

Porušení důvěrnosti/ integrity osobních údajů

Jiné (prosím upřesněte):

Škoda na majetku, zdraví

11. Kategorie dotčených osobních údajů?

- Osobní údaje Zvláštní kategorie (např. zdravotní/ genetické apod.):

Prosím upřesněte (např. jméno, příjmení, adresa, GPS lokalizace, platební údaje apod.):

12. Jaký je stav zašifrování dotčených osobních údajů?

- Kompletní
 Částečné
 Žádné

13. Byly dotčené osobní údaje předmětem Posouzení vlivu zpracování na ochranu osobních údajů? (DPIA)

- Ano Ne

14. Jaký způsob IT podpory společnost využívá?

- Interní IT team Externí IT firma

15. Jaká technická a organizační opatření byla přijata ke snížení následků porušení zabezpečení?

- Obnovení dat
 Vymazání škodlivého SW
 Výměna poškozeného nosiče
 Externí testování (např. Pentesting, etický hacker)
 Posílení bezpečnosti dat
 Školení zaměstnanců
 Jiné (prosím upřesněte):

16. Má společnost sjednané pojištění na daný typ incidentu?

- Ano

Prosím upřesněte:

- Ne

III. Doplňující informace

K vyplnění a sdílení s Dozorovým úřadem postupně bez dalšího zbytečného odkladu **od zjištění porušení zabezpečení.**

1. Datum/ čas ukončení následků útoku (ve formátu DD. MM. RRRR HH.MM):

2. Odhadovaná finanční škoda (Kč):

3. Kolik souborů osobních údajů bylo využito/ dotčeno/ zcizeno?

4. Bylo porušení zabezpečení osobních údajů oznámeno subjektům údajů?

 Ano Ne

5. Kolik subjektů údajů bylo informováno?

6. Odhadované finanční ztráty (Kč)

Náklady na oznámení:

Finanční újma:

7. Co bylo učiněno nebo naplánováno, aby oznámené porušení zabezpečení nenastalo znovu?

 Vylepšení bezpečnostních opatření s ohledem na bezpečnost dat, konkrétně: Audit and redesign shromažďování údajů Audit and redesign zpracování osobních údajů Audit and opětovné vyhodnocení Zpracovatele (pokud aplikovatelné) Zašifrování dat (at rest) Nebyla přijata bezpečnostní opatření Jiná technická a organizační opatření (prosím upřesněte):

8. Pokud je vám známo, jaká byla motivace za porušením zabezpečení v případě škodlivého útoku?

Malware

Ransomware

Phishing

SQL Injection Attack

Cross-site scripting (XSS)

Denial of Service (DoS)

Session hijacking

Credential reuse

Jiný (prosím upřesněte):

Dle Insurance Europe zpracoval: www.Cyberinsurance.cz