Šablona pro ohlašování případů porušení zabezpečení osobních údajů dozorovému úřadu

III DOPLŇUJÍCÍ INFORMACE K PORUŠENÍ ZABEZPEČNÍ

K vyplnění a sdílení s dozorovým úřadem ve lhůtě 4 týdnů od okamžiku, kdy se subjekt o porušení zabezpečení dozví.

III.1 Datum/čas ukončení následků útoku

III.2 Kolik osobních datových souborů bylo využívaných/dotčených/ukradených?

III.3 Byly subjekty údajů obeznámeny s porušením zabezpečení?

☐ Ano ☐ Ne

III.4 Kolik subjektů údajů bylo obeznámeno?

III.5 Odhadovaná finanční ztráta

Cena obeznámení

Finanční škoda

III.6 Jaká opatření byla podniknuta nebo plánována ke zmírnění pravděpodobnosti budoucího porušení zabezpečení?

☐ Posílení bezpečnostních opatření a především:
- ☐ Audit a přepracování procesu sběru dat
- ☐ Audit a přepracování procesu zpracování dat
- ☐ Audit a přehodnocení „zpracovatele" (lze-li aplikovat)
- ☐ Šifrování data at rest

☐ Žádná opatření nebyla přijata

☐ Jiné

III.7 Jste si vědomi příčiny porušení zabezpečení?

- ☐ Škodlivý útok
  - ☐ Interní ☐ Externí
- ☐ Nehoda (chyba v systému)
- ☐ Nedbalost (lidské pochybení)
- ☐ Jiná

III.8 Je-li známa, jaká byla motivace k porušení zabezpečení, jednalo-li se o škodlivý útok?

III.9 Je-li znám, jaký škodlivý software byl použit v případě škodlivého útoku?

- ☐ Útok prostředníka
- ☐ Malware
- ☐ Ransomware
- ☐ SQL Injection Attack
- ☐ Cross-site scripting (XSS)
- ☐ Denial of Service (DoS)
- ☐ Session hijacking
- ☐ Credential reuse
- ☐ Jiný