DS.12 Identity Theft or Fraud

Authors:

Last update: 2021-05-22 12:29:55 | By: Winfried Veil

Created at: 2021-05-12 09:14:17

Various GDPR provisions specify risk and damage categories, from which it can be derived which "rights and freedoms" it wants to protect, which risks it wants to avoid and which damage it wants to prevent.

Thus, it follows from Rec. 75 and 85 (1) GDPR that the GDPR also wants to prevent the occurrence of “identity theft” and “identity fraud”, because these could also be the consequence of the processing of personal data.

Identity theft is one of the top 15 cyber threats according to **ENISA**. Other cyber threats that may also be relevant for data protection and data security are not explicitly mentioned in the GDPR - such as malware, web-based attacks, web application attacks, phishing, denial of service, spam, botnets, insider threat, physical manipulation, damage, theft and loss, information leakage, cryptojacking, ransomware, cyber espionage.

However, fraud prevention may not only be an interest of the data subject, but also a legitimate interest of the controller **[Tile CO.22]**. Furthermore, the monitoring and prevention of fraud and tax evasion can also be a public interest, as **Rec. 71 (3) GDPR** larifies in the context of profiling and credit scoring. The multidimensionality of data processing is thus again reflected in the fact that fraud prevention can be an interest of the controller, an interest of the data subject and a public interest.