# INCIDENT HANDLING MANUAL FOR SUPPLIERS

# MANUÁL PRO ŘEŠENÍ INCIDENTŮ PRO DODAVATELE

## 1. DEFINITION OF INCIDENTS

An incident, in the context of data privacy and security of suppliers, refers to **any Supplier´s event or occurrence that compromises or is capable to compromise Deutsche Telekom Services Europe Czech republic s.r.o. (as the "Customer"), it´s integrity, confidentiality, or availability of information or systems.** Such incidents can involve unauthorized access to sensitive data, breaches of regulatory requirements, or actions that threaten the protection of personal information. They can lead to significant repercussions, including legal penalties, financial losses, operational disruptions, anti-social activities, and damage to an organization's reputation, necessitating prompt detection, response, and remediation efforts to mitigate risks and safeguard information assets.

### 1.1 SECURITY INCIDENTS

A security incident is an attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system or that measures put in place to protect them have failed. A security incident can also be any event that disrupts, or which could disrupt a service.

## 1. DEFINICE INCIDENTU

Incident v kontextu ochrany osobních údajů a bezpečnosti dodavatelů označuje **jakoukoli událost dodavatele, která ohrožuje nebo může ohrozit Deutsche Telekom Services Europe Czech Republic s.r.o. (jako "Zákazníka"), její integritu, důvěrnost nebo dostupnost informací či systémů.** Takové incidenty mohou zahrnovat neoprávněný přístup k citlivým údajům, porušení regulačních požadavků nebo jednání ohrožující ochranu osobních údajů. Mohou vést k významným následkům, včetně právních sankcí, finančních ztrát, provozních narušení, protispolečenských aktivit a poškození pověsti organizace, což vyžaduje rychlé odhalení, reakci a nápravu opatření ke snížení rizik a ochraně informačních aktiv.

### 1.1 BEZPEČNOSTNÍ INCIDENTY

Bezpečnostní incident je pokus o neoprávněný přístup, použití, zveřejnění, úpravu nebo zničení informací či narušení provozu systému v informačním systému, případně pokud selhala opatření zavedená na jejich ochranu. Bezpečnostní incident může být také jakákoli událost, která naruší nebo může narušit službu. Jinými slovy, incident je událost, která znemožní uživatelům pokračovat v každodenní

In other words, an incident is an event which disables users to continue their daily activity or have impact on performance of their work.

Examples of security incidents:

- Malware infection – the introduction of malicious software (e.g., viruses, ransomware, or spyware) into an organization's systems, which can harm data integrity or lead to unauthorized data access
- Social engineering attack (phishing/smishing/vishing) – a targeted attempt to steal sensitive information by masquerading as a trustworthy entity in electronic communications, often leading to compromised accounts
- Unauthorized access – gaining access to systems or data without proper authorization, which can happen through exploiting security vulnerabilities or using stolen credentials
- Physical security breach – unauthorized physical access to secure areas, such as data centres, which could lead to theft or damage to hardware and sensitive data
- Loss/Theft of company device – a company laptop or mobile device containing sensitive customer data is lost or stolen, leading to concerns about data exposure and potential identity theft

## 1.2 DATA PRIVACY INCIDENTS

A data privacy incident refers to any event that results in the unauthorized access, disclosure, loss, or alteration of personal data or information that is subject to privacy regulations. This can include incidents such as

činnosti nebo ovlivnit výkon jejich práce.

Příklady bezpečnostních incidentů:

- Infekce malwarem – zavedení škodlivého softwaru (např. viry, ransomware nebo spyware) do systémů organizace, který může poškodit integritu dat nebo vést k neoprávněnému přístupu k datům
- Útok sociálního inženýrství (phishing/smishing/vishing) – cílený pokus o krádež citlivých informací tím, že se v elektronické komunikaci vydává za důvěryhodnou entitu, což často vede ke kompromitovaným účtům
- Neoprávněný přístup – získání přístupu k systémům nebo datům bez řádného oprávnění, což může nastat zneužitím bezpečnostních zranitelností nebo použitím ukradených přihlašovacích údajů
- Fyzické bezpečnostní narušení – neoprávněný fyzický přístup do zabezpečených oblastí, jako jsou datová centra, který může vést ke krádeži nebo poškození hardwaru a citlivých dat
- Ztráta/krádež firemního zařízení – firemní notebook nebo mobilní zařízení obsahující citlivá zákaznická data je ztraceno nebo ukradeno, což vyvolává obavy z vystavení dat a možné krádeže identity

## 1.2 INCIDENTY TÝKAJÍCÍ SE OCHRANY OSOBNÍCH ÚDAJŮ

Incident týkající se ochrany osobních údajů označuje jakoukoli událost, která vede k neoprávněnému přístupu, zveřejnění, ztrátě nebo změně osobních údajů či informací, které podléhají předpisům o ochraně soukromí. To

data breaches, where unauthorized individuals gain access to sensitive data; accidental disclosure of personal information; or improper handling of data that violates privacy laws like the General Data Protection Regulation (GDPR). Data privacy incidents can lead to significant consequences, including legal penalties, financial harm, and damage to an organization's reputation, as well as potential harm to individuals whose data is compromised.

Examples of data privacy incidents:

- Data breach & misuse – an unauthorized third-party gains access to the company's database and steals sensitive personal information of customers
- Accidental data sharing or disclosure – an employee mistakenly sends an email containing personal data to the wrong recipient, exposing sensitive information to unauthorized individuals
- Social engineering attack (phishing/smishing/vishing) – employees fall victim to phishing schemes, inadvertently providing their login credentials or other sensitive information to cybercriminals, resulting in unauthorized access to the company's information systems
- Non-compliance with GDPR – The company fails to comply with GDPR principles, such as unauthorized data processing, e.g. obtaining proper consent for data processing, data minimization, or other issues leading to regulatory investigations and potential fines

může zahrnovat incidenty, jako jsou úniky dat, kdy neoprávněné osoby získají přístup k citlivým údajům; náhodné zveřejnění osobních údajů; nebo nesprávné nakládání s daty, které porušuje zákony o ochraně soukromí, jako je Obecné nařízení o ochraně osobních údajů (GDPR). Incidenty týkající se ochrany osobních údajů mohou vést k významným důsledkům, včetně právních sankcí, finančních škod a poškození pověsti organizace, stejně jako potenciální újmy pro jednotlivce, jejichž data jsou kompromitována.

Příklady incidentů týkajících se ochrany osobních údajů:

- Únik dat a zneužití – neoprávněná třetí strana získá přístup k databázi společnosti a ukradne citlivé osobní údaje zákazníků
- Náhodné sdílení nebo zveřejnění dat – zaměstnanec omylem pošle e-mail obsahující osobní údaje nesprávnému příjemci, čímž vystaví citlivé informace neoprávněným osobám
- Útok sociálního inženýrství (phishing/smishing/vishing) – zaměstnanci se stanou oběťmi phishingových schémat, kdy neúmyslně poskytují své přihlašovací údaje nebo jiné citlivé informace kyberzločincům, což vede k neoprávněnému přístupu k informačním systémům společnosti
- Nedodržení GDPR – Společnost nedodržuje zásady GDPR, jako je neoprávněné zpracování dat, např. získání řádného souhlasu se zpracováním dat, minimalizace dat nebo jiné problémy vedoucí k regulačním vyšetřováním a možným pokutám

## 2. INCIDENT REPORTING

Cases are reported to the local Data Privacy Officer (DPO)/Security Officer (SO). The local DPO and SO may also be contacted in case of questions or for consultancy. Suppliers shall report even in case they are not sure if it's an incident or already fixed the mistake. Incidents need to be reported without any delay.

## 3. INCIDENT PROCESS

1) Incident detection. Any Supplier can detect an incident. A concrete initial suspicion exists if facts are present or are plausibly asserted by a person giving a tip-off, which make misconduct, or a breach of obligations appear possible. All types of incidents must be reported.
2) Initial assessment and plausibility check by the local Security or Data Protection Officer. If the incident is found plausible the investigation phase starts.
3) Investigation and impact assessment is done with the help of impacted departments, depending on incident type. The first point of contact is the local responsible Data Privacy or Security Officer.
4) Mitigation and documentation. Any immediate measure resulted from the investigation and impact assessment shall be launched. The responsible Officer shall continuously document relevant incidents and the measures taken in conjunction with them.
5) Close case

## 2. INCIDENT REPORTING

Případy jsou hlášeny místnímu Data Privacy Officer (DPO)/Security Officer (SO). Místní DPO a SO lze také kontaktovat v případě dotazů nebo pro konzultace. Dodavatelé by měli nahlásit i v případě, že si nejsou jisti, zda šlo o incident nebo chybu již opravili. Incidenty je třeba hlásit bez jakéhokoliv prodlení.

## 3. PROCES INCIDENTU

1) Detekce incidentu. Konkrétní počáteční podezření existuje, pokud jsou přítomny skutečnosti nebo jsou věrohodně tvrzeny osobou poskytující tip, které naznačují, že je možné porušení povinností nebo protiprávní jednání. Všechny typy incidentů musí být hlášeny.
2) Počáteční posouzení a ověření věrohodnosti místním Security nebo Data Privacy Officer. Pokud je incident shledán věrohodným, začíná fáze vyšetřování.
3) Vyšetřování a posouzení dopadů probíhá s pomocí postižených oddělení v závislosti na typu incidentu. Prvním kontaktním místem je místní Data Privacy nebo Security Officer.
4) Zmírnění škod a dokumentace. Jakékoli okamžité opatření vyplývající z vyšetřování a posouzení dopadů bude zahájeno. Odpovědný Officer bude průběžně dokumentovat příslušné incidenty a opatření, která s nimi souvisí.
5) Uzavření případu

## 4. INCIDENT CATEGORIES

| Type of Incident | Identification |
|---|---|
| Malware infection | Security |
| Social engineering attack (phishing/smishing/vishing) | Security<br>Data Privacy |
| Unauthorized access | Security |
| Physical security breach | Security |
| Loss/Theft of company device | Security |
| Loss/Theft of employees personal belongings | Security |
| Loss/Theft of entry cards | Security |
| Data breach & misuse | Data Privacy |
| Accidental data sharing or disclosure | Data Privacy |
| Non-compliance with GDPR | Data Privacy |

## 4. KATEGORIE INCIDENTŮ

| Typy incidentů | Identifikace |
|---|---|
| Infekce malwarem | Bezpečnost |
| Útok sociálním inženýrstvím (phishing/smishing/vishing) | Bezpečnost<br>Ochrana osobních údajů |
| Neoprávněný přístup | Bezpečnost |
| Fyzické narušení bezpečnosti | Bezpečnost |
| Ztráta/krádež firemního zařízení | Bezpečnost |
| Ztráte/krádež osobních věcí zaměstnanců | Bezpečnost |
| Ztráta/krádež přístupových karet | Bezpečnost |
| Únik a zneužití osobních údajů | Ochrana osobních údajů |
| Náhodné sdílení osobních dat nebo jejich zveřejnění | Ochrana osobních údajů |
| nedodržení GDPR | Ochrana osobních údajů |

## 5. CONTACTS

| | |
|---|---|
| Security Officer | jakub.misinger@telekom.com |
| Data Privacy Officer | jakub.misinger@telekom.com |

## 5. KONTAKTY

| | |
|---|---|
| Security Officer | jakub.misinger@telekom.com |
| Data Privacy Officer | jakub.misinger@telekom.com |

.