Mitteilung einer unrechtmäßigen Datenübermittlung bzw. unrechtmäßigen Kenntniserlangung von Daten durch Dritte („Datenpanne“) gemäß Art. 33 Abs. 1 DSGVO oder § 15a TMG i.V.m. §42a BDSG

Hinweise:

Bei bestimmten Datenschutzverstößen und Datenschutzpannen müssen die Sie als verantwortliche Stelle die zuständige Datenschutzaufsichtsbehörde in Nordrhein-Westfalen oder Rheinland Pfalz (www.datenschutz-wiki.de/Aufsichtsbeh%C3%B6rden_und_Landesdatenschutzbeauftragte LINK) und die betroffenen Personen innerhalb von 72 Stunden nach Bekanntwerden des Verstoßes gem. Art. 33 Abs. 1 DSGVO oder § 15a TMG i.V.m. §42a BDSG informieren. (Hinweis: In der Regel werden hier auch beschreibbare PDFs auf den Seiten der Landesdatenschutzbeauftragten vorgehalten.)

Eine solche „Verpflichtung zur Selbstanzeige“ besteht, wenn Dritte unrechtmäßig von bestimmten sensiblen Daten Kenntnis erlangt haben und schwerwiegende Beeinträchtigungen für die Rechte oder schutzwürdigen Interessen der betroffenen Personen drohen.

Voraussetzungen für die Informationspflicht

Die Informationspflicht tritt ein, wenn folgende in der Datenschutzgrundverordnung abschließend genannten Arten personenbezogener Daten von einem Datenschutzverstoß bzw. einer Datenpanne betroffen sind:

- besondere Kategorien personenbezogener Daten gemäß Art. 9 Abs. 1 DSGVO, z.B. Gesundheitsdaten oder Religionszugehörigkeit,
- personenbezogene Daten, die z.B. bei Ärzten, Apothekern, Rechtsanwälten, Steuerberatern oder Personenversicherern einem Berufsgeheimnis unterliegen,
- personenbezogene Daten, die sich auf strafbare Handlungen oder Ordnungswidrigkeiten oder auf einen Verdacht hierauf beziehen,
- personenbezogene Daten zu Bank- und Kreditkartenkonten, z.B. Kontonummern mit Bankleitzahl oder Kreditkartennummern und
- Bestands- und Nutzungsdaten im Bereich der Telemedien (Internet), z.B. Benutzerkennungen, Passworte.

Die unrechtmäßige Kenntniserlangung von Daten durch Dritte kann auf einer unrechtmäßigen Übermittlung von Daten beruhen (z.B. Fehl-Versendungen, illegale Datenweitergaben oder Datenabrufe). Die Daten können aber auch auf sonstige Weise dritten Personen unrechtmäßig zur Kenntnis gelangen, insbesondere beim Verlust von Datenträgern durch Einbrüche, Diebstähle und Fundunterschlagungen oder beim Internet-Datenhacking.

Es muss nicht im Einzelfall schon belegt sein, dass dritte Personen von den Daten tatsächlich Kenntnis erlangt haben, z.B. durch bereits eingetretene Schadensfälle wie illegale Lastschrifteinzüge von Bankkonten oder Internetbestellungen auf Kosten der Geschädigten. Es reicht aus, dass aufgrund der Lebenserfahrung eine hohe Wahrscheinlichkeit dafür besteht, dass die Daten von einem Dritten zur Kenntnis genommen wurden bzw. werden. Dies ist insbesondere gegeben, wenn Daten durch eine kriminelle Handlung in den Verfügungsbereich Dritter gelangt sind. Denn dann besteht eine hohe Wahrscheinlichkeit dafür, dass z.B. Diebe, Cyberkriminelle oder ihre Abnehmer die gespeicherten Daten für rechtswidrige Zwecke nutzen, womit für die Betroffenen eine konkrete Gefahr droht.

Bei der Frage, ob schwerwiegende Beeinträchtigungen für die Rechte oder schutzwürdigen Interessen der betroffenen Personen drohen, ist eine Prognoseentscheidung zu treffen, ob eine schwerwiegende Beeinträchtigung in eine bedrohliche Nähe gerückt ist. Dabei ist zu berücksichtigen, um welche Art von Daten es geht, wer - vermutlich - in den Besitz der Daten gelangt ist ("vertrauenswürdige Umgebung" oder kriminelle Personen) und welche potentiellen Auswirkungen sich für die betroffenen Personen ergeben können, z.B. finanzielle Schäden, Identitätsbetrug, soziale Nachteile, Bloßstellung, Erpressbarkeit.

Umsetzung der Informationspflicht

Die verantwortliche Stelle muss innerhalb von 72 Stunden nach Bekanntwerden des Datenschutzverstoßes gem. Art. 33 Abs. 1 DSGVO oder § 15a TMG i.V.m. §42a BDSG die zuständige Datenschutzaufsichtsbehörde und unverzüglich die betroffenen Personen, um deren Daten es geht, gem. Art. 34 Abs. 1 DSGVO informieren, wenn ein hohes Risiko für die persönlichen Rechte und Freiheiten der Betroffenen durch den Verstoß vorliegt. Dabei muss sie mitteilen, was konkret geschehen ist, welche Maßnahmen zur Abhilfe inzwischen getroffen wurden und was die betroffenen Personen selbst für ihren Schutz noch tun können.

Die zuständige Datenschutzaufsichtsbehörde kann nach der Information prüfen, ob die meldende Stelle die möglichen bzw. gebotenen Abhilfe-, Schutz- und Sicherheitsmaßnahmen schon getroffen hat und bei Bedarf weitere Maßnahmen einfordern.

Die Information der betroffenen Personen muss folgenden Inhalt haben:

- Name der verantwortlichen Stelle mit Ansprechpartnern und Kontaktdaten,
- Datum/Zeitraum des Vorfalls sowie Ursache der Datenpanne (kurze Beschreibung des Sachverhalts) mit Beschreibung der betroffenen personenbezogenen Daten,
- Nennung der (möglichen) Dritten, die Kenntnis erlangt haben bzw. die eine Möglichkeit zur Kenntnisnahme hatten,
- mögliche Folgen bzw. nachteilige Auswirkungen der Datenpanne (z.B. finanzieller Schaden, Ruf-/Imageschädigung, Bloßstellung) mit Hinweisen auf mögliche Vorkehrungen der betroffenen Personen dazu, und
- infolge der Datenpanne durch die verantwortliche Stelle ergriffene Maßnahmen.

Aufgrund der Information sollen die betroffenen Personen die Möglichkeit haben, Schaden von sich abzuwenden oder Schutzmaßnahmen zu treffen.

Ein Verstoß gegen die Informationsverpflichtung gegenüber der Datenschutzaufsichtsbehörde oder den betroffenen Personen ist bußgeldbewehrt (Art. 83 Abs. 4a DSGVO).

Für den Fall bekannt werdender Datenpannen sollte die verantwortliche Stelle organisatorisch gerüstet sein und ein geeignetes Prüfungs- und Meldesystem vorbereitet haben.

§ 1 Meldebogen für Datenschutz- und Sicherheitsereignisse

Ereignisnummer:	Vertraulichkeitskennzeichnung	gemeldet am:	Status:
Ereignisdatum:	gemeldet von:		Priorität hoch
verantwortlicher Bearbeiter:	Kategorie: □ Datenschutz □ Informationssicherheit □ IT-Sicherheit □ Andere:		
Ausführliche Beschreibung:			
betroffene Komponenten:	System:	Standort:	verantwortliche Abteilung:

Sofortmaßnahmen:	Effekt in Prozent:	Einführungsdatum:
Fehlerursachen: Ursachen:	Effekt in Prozent:	Einführungsdatum:
geplante Korrektivmaßnahmen: Maßnahmen:	kontrolliert durch:	Kontrolldatum:
Information an Betroffene □ nötig □ nicht nötig. Begründung: Art (E-Mail/Fax/Brief): Datum:		

□ Datenschutzbeauftragte/r eingebunden Begründung:	□ Behörde eingebunden Begründung:

§ 2 Priorisierungstabelle

Mit der Priorisierungstabelle erfolgt die Festlegung der Priorität. Für eine einfache und übersichtliche Priorisierung wird mit vier Prioritäten gearbeitet (Auswirkung/Schaden): katastrophal und existenzbedrohlich (1), großer Schaden (2), mittlerer Schaden (3), geringer Schaden (4).

Durch die Bestimmung der Kategorie und deren Auswirkung wird eine Priorisierung des Datenschutzereignisses gemäß nachfolgender Tabelle abgeleitet:

Kategorie	*geringe Auswirkung/ Schaden*	*mittlere Auswirkung/ Schaden*	*große Auswirkung/ Schaden*	*katastrophale Auswirkung/ Schaden*
Diebstahl von Kundendaten				
Verletzung des Datenschutzes				
Verstoß gegen Gesetze				
Hackerangriff				

Um die Priorisierung und die damit zusammenhängenden Ereignisse zuordnen zu können, ist das Arbeiten mit entsprechenden tabellarischen Übersichten geeignet. Beispielhaft sind nachfolgend die Ereignisse aus der oben dargestellten Tabelle beschrieben.

Diebstahl von personenbezogenen Daten		
Auswirkung		*Priorität*
gering	nicht klassifizierte Personendaten wurden unautorisiert kopiert	
mittel	vertrauliche Personendaten wurden unautorisiert kopiert	
groß	vertrauliche Personendaten werden veröffentlicht; Schadensersatzforderungen von Betroffenen möglich; Mitteilung nach § 42 a BDSG notwendig;	
katastrophal	sensible Personendaten werden veröffentlicht; sehr hohe Schadensersatzforderungen von Betroffenen möglich; Meldung nach § 42 a BDSG notwendig; Imageschaden für das Unternehmen	

Verletzung des Datenschutzes		
Auswirkung		*Priorität*
gering	versehentliche Weitergabe von personenbezogenen Daten innerhalb des Unternehmens	
mittel	unbeabsichtigte personenbezogene Daten in Auswertungen; personenbezogene Daten ohne Zweckbindung in Log-Dateien	
groß	grob fahrlässige Offenbarung personenbezogener Daten gegenüber Dritten, Verletzung des Trennungsgebots; Informationspflicht nach § 42 a BDSG notwendig	
katastrophal	Veröffentlichungen von personenbezogenen Daten; Zweckmissbrauch Diebstahl von personenbezogenen Daten; Unerlaubte Nutzung von personenbezogenen Daten zur Verhaltenskontrolle Informationspflicht nach § 42 a BDSG notwendig	

Verstoß gegen Gesetze		
Auswirkung		*Priorität*
gering	geringfügiger Verstoß gegen den Datenschutz ohne erkennbaren Vorsatz keine Außenwirkung Vorfall kann intern (ggf. mit disziplinarischen Mitteln) geregelt werden	
mittel	Ordnungswidrigkeit mittelschwerer Verstoß gegen den Datenschutz Einsatz zwingender disziplinarischer Mittel erforderlich Prüfung der Hinzuziehung der entsprechenden Behörden notwendig möglicherweise Informationspflicht nach § 42 a BDSG notwendig	
groß	Rechtsverstoß Hinzuziehung der entsprechenden Behörden notwendig Informationspflicht nach § 42 a BDSG notwendig	
katastrophal	strafrechtliche Relevanz mit eindeutig erkennbarem Vorsatz Einschaltung der Strafermittlungsbehörden zwingend erforderlich hohe Außenwirkung mit Imageverlust für das Unternehmen Informationspflicht nach § 42 a BDSG notwendig	

Hackerangriff		
Auswirkung		*Priorität*
gering	Angriff auf IT-Systeme mit personenbezogenen Daten Angriff ohne nachweislichen Schaden (z. B. Versuch eines Hackereinbruchs wird rechtzeitig erkannt und vereitelt)	
mittel	Angriff mit geringfügiger Verschlechterung der Verfügbarkeit Angriff auf die IT-Infrastruktur wird durch entsprechende technische Frühwarnsysteme erkannt und führt zur vorübergehenden Sicherheitsabschaltung dezidierter Systeme oder Segmente	
groß	Hackerzugriff auf zentrale Verarbeitungssysteme Diebstahl von Passwortdateien massive Beeinträchtigungen der Dienste Hinzuziehung der entsprechenden Behörden notwendig Informationspflicht nach § 42 a BDSG notwendig	
katastrophal	Ausfall von Systemen durch Hackerangriffe Verlust von Daten durch Hacker Diebstahl von personenbezogenen Daten Offenlegung von personenbezogenen Daten durch Hacker hohe Außenwirkung mit Imageverlust für das Unternehmen Einschaltung der Strafermittlungsbehörden zwingend erforderlich Informationspflicht nach § 42 a BDSG notwendig	