



Dienstanweisung Nr. 58/2018 zum Umgang mit Datenschutzvorfällen

1. Änderung vom 18.09.2023

Inhalt

Präambel.....	3
§ 1 Ziele	3
§ 2 Geltungsbereich	3
§ 3 Aufgaben des Datenschutzmanagementteams	3
§ 4 Interner Meldeablauf.....	4
§ 5 Externer Meldeablauf	4
§ 6 Hinweise zu den Meldungen.....	4
§ 7 Registerführung/Ablage	5
§ 8 Inkrafttreten	5

Präambel

Diese Dienstanweisung dient der Strukturierung und Steuerung des kreislichen Handels bei Vorfällen, die tatsächlich oder möglicherweise ein Risiko für das Recht auf informationelle Selbstbestimmung darstellen. Ein solches Risiko kann entstehen, wenn Vorgaben der IT-Sicherheit oder des Datenschutzrechts verletzt werden.

§ 1 Ziele

Ziele dieser Anweisung sind:

- die Erfassung und Bewertung möglicher Datenschutzvorfälle
- die Vorbereitung einer ggf. notwendigen Mitteilung an die Aufsichtsbehörde (Art. 33 DSGVO bzw. § 65 BDSG) unter Einhaltung der vorgeschriebenen 72-Stunden-Frist,
- die Vorbereitung einer ggf. notwendigen Mitteilung an die betroffene/n Person/en (Art. 34 DSGVO bzw. § 66 BDSG)
- die Dokumentation sämtlicher Vorkommnisse sowie
- die Festlegung von Maßnahmen, die die Risiken für das Grundrecht auf informationelle Selbstbestimmung abwenden oder minimieren.

§ 2 Geltungsbereich

Diese Dienstanweisung richtet sich an tariflich Beschäftigte, Beamt*innen, Auszubildende, Studierende und Referendar*innen des Landkreises, nachfolgend Beschäftigte genannt.

Sie gilt nicht für Beschäftigte des Jobcenters.

Diese Dienstanweisung greift bei Datenschutzvorfällen¹ der allgemeinen Verwaltung (hier DSGVO) und in Bußgeldverfahren (hier Teil 3 des BDSG).

§ 3 Aufgaben des Datenschutzmanagementteams

Die zuständigen Beschäftigten im Amt für zentrale Steuerung, Organisation und Personal bilden das Datenschutzmanagementteam (DSM-Team). Aufgaben des DSM-Teams sind:

- das Meldeverfahren zu begleiten,
- auf die Wahrung der gesetzlichen Fristen hinzuwirken,
- den betroffenen Fachbereichen inhaltliche Hilfestellungen zu geben,
- die Endredaktion des Meldebogens,
- nach Bedarf die/den Datenschutzbeauftragten und die/den IT-Sicherheitsbeauftragten einzubeziehen,
- die Registerführung entsprechend § 7,
- die ergriffenen Maßnahmen zu dokumentieren, um die festgestellten Mängel für die Zukunft zu reduzieren.

¹ Gemäß Artikel 4 Nr. 12 DSGVO stellt die Verletzung des Schutzes personenbezogener Daten eine Verletzung der Sicherheit dar, die zur Vernichtung, zum Verlust, zur Veränderung oder zur unbefugten Offenlegung von beziehungsweise zum unbefugten Zugang zu personenbezogenen Daten führt, die übermittelt, gespeichert oder auf sonstige Weise verarbeitet wurden. Dies gilt unabhängig davon, ob die Verletzung unbeabsichtigt oder unrechtmäßig war.

§ 4 Interner Meldeablauf

Jede - auch nur mögliche - Datenschutzverletzung ist von dem/der Beschäftigten an die nächste Führungskraft zu melden. Diese informiert per Vorabmeldung (Anlage 1) unverzüglich auf dem Dienstweg das Büro der Landrätin und parallel das Datenschutzmanagementteam (DSM-Team@teltow-flaeming.de).

Das DSM-Team vergibt ein Aktenzeichen und informiert ggf. den/die Datenschutzbeauftragte/n und den/die IT-Sicherheitsbeauftragte/n.

Daraufhin ist der Meldebogen (Anlage 2) binnen 24 Stunden durch den Fachbereich zu erstellen und an das DMS-Team weiterzuleiten.

Zur vollständigen Sachverhaltsdarstellung sind im Bedarfsfalle anonymisierte Kopien verfahrensrelevanter Dokumente an das DSM-Team zu übermitteln.

Handelt es sich um einen meldepflichtigen Datenschutzvorfall leitet das DSM-Team den ggf. überarbeiteten Meldebogen zu Unterschrift und zum Postausgang an die in § 5 benannte Stelle weiter.

Eine Kopie des unterschriebenen Dokuments ist an das DSM-Team zur Ablage zu übermitteln.

§ 5 Externer Meldeablauf

Eine Meldung an die Aufsichtsbehörde nach Art. 33 DSGVO bzw. § 65 BDSG erfolgt bei Datenschutzverstößen

- a) im Bereich der Landrätin durch die Hauptverwaltungsbeamtin
- b) im Bereich des Jugend- bzw. Sozialamtes durch die jeweilige Amtsleitung²
- c) im sonstigen Bereich des Dezernates II durch die Dezernatsleitung
- d) in den Bereichen der übrigen Dezernate durch die jeweilige Dezernatsleitung

Ist eine Benachrichtigung an den oder die Betroffenen notwendig (Art. 34 DSGVO bzw. § 66 BDSG) erfolgt diese ebenfalls durch die benannte Stelle.

Zur besseren Übersicht enthält Anlage 5 eine visuelle Darstellung des vollständigen Meldeablaufs.

§ 6 Hinweise zu den Meldungen

In sämtlichen Dokumenten sind Namen der beteiligten Personen nicht zu nennen.

Handelt es sich um Vorfälle, die sich durch eingesetzte IT-Systeme ereignet haben, ist darauf konkret in der Vorabmeldung und im Meldebogen hinzuweisen. Das DSM-Team bezieht dann neben dem/der IT-Sicherheitsbeauftragte/n auch das Amt für Digitalisierung und Informationstechnik ein.

Je nach Schwere des Eingriffs und der möglichen Folgen der Datenschutzverletzung kann eine unverzügliche Benachrichtigung der betroffenen Person/en notwendig werden. Ist die Abwendung oder Minimierung des Risikos nur durch eine Handlung der betroffenen Person/en

² (entsprechend § 67 Abs. 4 SGB X)

erreichbar, ist daher der Kontakt zu der/den betroffenen Person/en bereits dann zu suchen, wenn der interne und externe Meldeablauf noch nicht erfolgt bzw. abgeschlossen ist.

Eine entsprechende Information des/der Betroffenen ist i.d.R. bei der Verletzung des Schutzes von besonderen Kategorien personenbezogener Daten notwendig. Sie kommt außerdem in Betracht, wenn eines der folgenden Kriterien erfüllt ist:

- Diskriminierung,
- Identitätsdiebstahl/-betrug,
- Verletzung des Berufsgeheimnisses,
- Aufhebung einer Pseudonymisierung,
- negative finanzielle Auswirkungen.

In Bußgeldverfahren sind die Bestimmungen des § 66 Abs. 5 BDSG zu beachten.

Zur schriftlichen Benachrichtigung können die in der Anlage 4 aufgeführten Formulierungsvorschläge verwendet werden. Ein persönliches Gespräch ist nur auf Verlangen der betroffenen Person möglich (Artikel 12 Abs. 1 DSGVO). Die öffentliche Bekanntmachung oder ähnliche Maßnahmen kommen nur bei Benachrichtigungen mit unverhältnismäßigem Aufwand in Betracht. Allenfalls ist die Mindestangabe der in Artikel 33 Absatz 3 Buchstabe b, c und d genannten Informationen und Maßnahmen sicherzustellen.

§ 7 Registerführung/Ablage

Die Dokumentation sämtlicher Vorkommnisse wird über eine zentrale Registerführung durch das DSM-Team realisiert. Die Ablage im betroffenen Fachbereich erfolgt nach Bedarf in separaten Sachakten und nicht in der Verfahrensakte.

Nach Abschluss des Verfahrens werden die Unterlagen 3 Jahre aufbewahrt.

§ 8 Inkrafttreten

Die 1. Änderung der Dienstanweisung tritt am Tag nach Intranetveröffentlichung in Kraft.

Luckenwalde, den 18.09.2023

Wehlan
Landrätin

Anlage 1 – Vorabmeldung
Anlage 2 – Meldebogen
Anlage 3 – Anschreiben LDA (Muster)
Anlage 4 – Formulierungsvorschläge
Anlage 5 – Meldeablauf

Vorabmeldung

Bitte unverzüglich an das Büro der Landrätin und an das Datenschutzmanagementteam übermitteln (DSM-Team@teltow-flaeming.de), ggf. zusätzlich telefonisch informieren.

Hinweis:

Beteiligte Personen sind namentlich **nicht** zu nennen, nutzen Sie bitte Funktionsbezeichnungen wie Antragsteller*in, Sachbearbeiter*in, Rechtsbeistand, Bevollmächtigte*r, Führungskraft etc.

betroffener Fachbereich

Kurzdarstellung des Vorfalls

Einschätzung zur Meldepflicht Art. 33 DSGVO bzw. § 65 BDSG

- ☐ Liegen Anhaltspunkte dafür vor, dass die Verletzung voraussichtlich **nicht** zu einem Risiko für die Rechte und Freiheiten natürlicher Personen führt?
Kurze Begründung:

Einschätzung zur Benachrichtigungspflicht Art. 34 DSGVO bzw. § 66 BDSG

- ☐ Liegt ein **hohes** Risiko für den Betroffenen vor und ist eine unverzügliche Benachrichtigung erforderlich bzw. bereits erfolgt?

Wenn nicht, warum?
Kurze Begründung:

Meldebogen (zur Übermittlung an die Aufsichtsbehörde)

Art der Meldung

☐ vorläufig

☐ Ergänzung zur Meldung vom:

☐ vollständig

Meldung einer Datenschutzverletzung

Aktenzeichen

Absender

Landkreis Teltow-Fläming

Bitte auswählen

Am Nuthefließ 2

14943 Luckenwalde

Telefon: 03371/608-

E-Mail:

Behördlicher Datenschutzbeauftragter

Franco Capalbo

Telefon: 03371/608-1308

E-Mail: datenschutz@teltow-flaeming.de

1. Sachverhaltsdarstellung

Sachverhaltsdarstellung (bitte keine Namen der beteiligten Person/en aufführen)

2. Zeitliche Abfolge

Zeitpunkt des Vorfalls

Dauert der Vorfall noch an?

Ist eine Wiederholung zu befürchten?

Wer hat den Vorfall festgestellt und wann?

Falls die Meldung nicht innerhalb von 72 Stunden nach Feststellung des Vorfalls erfolgt ist.
Begründung für die Verzögerung:

3. Personen- bzw. Datenkategorien (Mehrfachnennungen möglich)

Von der Verletzung betroffene Person/en:

- | | |
|---|---|
| ☐ Antragsteller*in | ☐ Führungskraft |
| ☐ Beschäftigter*in | ☐ Lieferanten |
| ☐ Personensorgeberechtigte*r | ☐ Rechtsbeistand |
| ☐ Bewerber | ☐ weitere |

Anzahl der betroffenen Person/en:

Welche personenbezogenen Daten sind betroffen?

- | | |
|--|---|
| ☐ Name, Vorname | ☐ Bankdaten |
| ☐ Anschrift | ☐ Logindaten |
| ☐ Geburtsdatum | ☐ Protokolldaten |
| ☐ sonstige Kontaktdaten | ☐ weitere |

Sind folgende personenbezogene Daten besonderer Kategorien betroffen?

- ☐ rassische und ethnische Herkunft
- ☐ politische Meinung
- ☐ religiöse oder weltanschauliche Überzeugung
- ☐ Gewerkschaftszugehörigkeit
- ☐ Daten zum Sexualleben oder der sexuelle Orientierung
- ☐ genetische Daten
- ☐ biometrische Daten
- ☐ Gesundheitsdaten
- ☐ noch nicht bekannt, da:

Art der Datenschutzverletzung (Mehrfachnennungen möglich)

- ☐ Vernichtung/Verlust
- ☐ Veränderung
- ☐ unbefugte Offenlegung
- ☐ unbefugter Zugriff

Anzahl der betroffenen Datensätze

4. Folgen der Datenschutzverletzung: (Zutreffendes bitte ankreuzen bzw. erläutern)

Welche Folgen für die Sicherheit der Datenverarbeitung sind eingetreten?

- ☐ Verlust der Vertraulichkeit der Daten (z. B. durch unbefugte Offenlegung von bzw. unbefugten Zugang zu Zugang zu personenbezogenen Daten

Welche Folgen für die Sicherheit der Datenverarbeitung sind eingetreten?

- ☐ Verlust der Integrität (z. B. durch Veränderung der Daten)
- ☐ Einschränkung bzw. Verlust der Verfügbarkeit der Daten (z. B. durch Löschung oder Verschlüsselung der Daten)

Welche sonstigen Folgen für die Sicherheit der Datenverarbeitung sind eingetreten?

Mögliche negative Folgen für die betroffenen Personen (Mehrfachnennungen möglich)

- | | |
|---|--|
| ☐ Diskriminierung | ☐ Geheimnisoffenbarung |
| ☐ Identitätsdiebstahl oder –betrug | ☐ unbefugte Aufhebung von Pseudonymisierung |
| ☐ Finanzieller Schaden | ☐ gesellschaftliche Nachteile |
| ☐ Rufschädigung | ☐ wirtschaftliche Nachteile |
| ☐ Existenzgefährdung | ☐ Gefahr für Leib- und Leben |
| ☐ Verlust des Arbeitsplatzes | ☐ sonstige: |

5. Beschreibung der ergriffenen und/oder geplanten technischen und organisatorischen Maßnahmen, die sicherstellen, dass der Vorfall beendet ist und in Zukunft nicht erneut auftreten wird:

bereits umgesetzte Maßnahmen

geplante Maßnahmen (Bitte möglichst einen genauen Zeitplan angeben)

Begründung in dem Fall, dass keine Maßnahmen eingeleitet wurden oder werden

6. Benachrichtigung der betroffenen Person/en: (falls erforderlich)

Die Information des*der Betroffenen ist bereits erfolgt bzw. wird erfolgen,

- ☐ ja, am:
- ☐ nein (nur wenn die Verletzung des Schutzes personenbezogener Daten voraussichtlich nicht zu einem Risiko für die Rechte und Freiheiten natürlicher Personen führt)

Begründung:

Anzahl der zu benachrichtigten Personen

Art und Weise der Information

- ☐ Anschreiben

Art und Weise der Information

- ☐ persönliches Gespräch
- ☐ öffentliche Bekanntmachung, o.ä.
- ☐ sonstiges:

Landkreis Teltow-Fläming

Die Landrätin

MUSTER



Kreisverwaltung Teltow-Fläming • Am Nuthefließ 2 • 14943 Luckenwalde

Bereich

Dienstgebäude: Am Nuthefließ 2

Landesbeauftragte für den Datenschutz und
das Recht auf Akteneinsicht
Frau Dagmar Hartge
Stahnsdorfer Damm 77
14532 Kleinmachnow

Auskunft:
Zimmer:
Telefon: 03371 608-
Telefax: 03371 608-
E-Mail:
Datum:

Vorab per Fax: 033203/35649

(ggf: Vorläufige) Meldung eines Datenschutzvorfalls nach Artikel 33 DSGVO – Aktenzeichen

Sehr geehrte Frau Hartge,

ich übersende Ihnen den Meldebogen zu einem Datenschutzvorfall in der Kreisverwaltung Teltow-Fläming. Konkret handelt es sich dabei um (*Benennung der Datenschutzverletzung*) im Sachgebiet ... des Amtes ...

oder

in der Kreisverwaltung Teltow-Fläming kam es (möglichweise) zu einem Datenschutzvorfall. Dabei könnte es sich um (*Benennung der Datenschutzverletzung*) handeln, welche sich im Amt ... ereignete. Sobald die Ermittlungen abgeschlossen sind, wird Ihnen der vollständige Meldebogen zugesandt.

Mit freundlichen Grüßen

zuständige Stelle

* Die genannte E-Mail Adresse dient nur zum Empfang einfacher Mitteilungen ohne Signatur und/oder Verschlüsselung
Öffnungszeiten:

Dienstag 09:00 - 12:00 Uhr und 13:00 - 15:00 Uhr
Donnerstag 09:00 - 12:00 Uhr und 13:00 - 17:30 Uhr

Telefon: 03371 608-0
Telefax: 03371 608-9100
UST-IdNr.: DE162693698

Bankverbindung:
Mittelbrandenburgische Sparkasse in Potsdam
Gläubiger-ID: DE 87 LTF 000 002 134 52
BIC: WELADED1PMB
IBAN: DE86 1605 0000 3633 0275 98

Einzelne Beratungsdienste haben andere Öffnungszeiten. Diese erfahren Sie über die Telefonzentrale oder im Internet.
Sie können Ihr Anliegen nach Absprache mit dem Mitarbeiter auch Mo, Di, Mi, Do bis 19:00 Uhr und Fr bis 16:00 Uhr in der Kreisverwaltung erledigen.

Internet: <http://www.teltow-flaeming.de>

Anlage 4 – zur DA 58/18

Formulierungsvorschläge zur Benachrichtigung der von einer Verletzung des Schutzes personenbezogener Daten betroffenen Personen (Art. 34 DSGVO bzw. § 66 BDSG)

1. Benennung der konkreten Datenschutzverletzung im Betreff:

- Weitergabe Ihrer Daten durch...
- Postfehlversendung vom...
- Unbefugter Datenzugriff (Cyberattacke) am...

2. Sachverhaltsdarstellung ggf. aus Meldebogen übernehmen und schlussfolgern:

Im Sachgebiet ... des Amtes ... wurde eine E-Mail bedauerlicherweise an einen falschen Adressaten versandt.

Dadurch ist es zur unbefugten Offenlegung Ihrer folgenden personenbezogenen Daten gekommen: - Name, Anschrift
- ...

3. Darlegung der bereits ergriffenen Maßnahmen:

- Unmittelbar nach Kenntnisnahme wurde die fehlgeleitete E-Mail gelöscht
- Sämtliche Internetverbindungen wurden umgehend getrennt
- Die Unterlagen wurden zurückgegeben

4. Benennung möglicher Risiken und Erläuterung:

- Identitätsmissbrauch
- Finanzielle Verluste
- Diskriminierung

5. Empfohlene Maßnahmen im Falle eines Hackerangriffs:

- Achten Sie auf Auffälligkeiten, die auf einen Missbrauch Ihrer Daten hinweisen könnten.
- Beobachten Sie sämtliche Geldbewegungen auf Ihren Bankkonten
- Melden Sie sämtliche Auffälligkeiten, die auf einen Identitätsmissbrauch hindeuten

6. Schlussformulierung:

Für den Vorfall und den damit in Zusammenhang stehenden Unannehmlichkeiten bitte ich um Entschuldigung. Bei Fragen können Sie sich gern melden.

Freundliche Grüße

zuständige Stelle

Anlage 5 – Meldeablauf

