DATENSCHUTZSTELLE
FÜRSTENTUM LIECHTENSTEIN

Datenschutz-Grundverordnung (DSGVO) «Spickzettel» für die Praxis/Technik

Der gegenständliche «Spickzettel» richtet sich insbesondere an Personen, die sich für die automatisierte Datenverarbeitung im engeren Sinn (Betreuung der datenverarbeitenden IT-Infrastruktur, Implementierung geeigneter technischer und organisatorischer Massnahmen (**TOM**s) usw.) verantwortlich zeichnen. Der Spickzettel ist sehr stark auf Kernaussagen und Grundsätze reduziert. Ergänzende *Erläuterungen* oder *Ausnahmeregelungen* in den einzelnen Bestimmungen der DSGVO *bleiben – im Sinne der Lesbarkeit und Kürze – vielerorts unerwähnt*. In den Endnoten finden sich entsprechende Verweise. Das Dokument erhebt *keinen Anspruch auf Vollständigkeit*. Anregungen und Verbesserungen nimmt die Datenschutzstelle (**DSS**) jederzeit gerne entgegen. Weitere Informationen finden sich unter https://www.datenschutzstelle.li/.

Begriffsbestimmungen

«**Personenbezogene Daten**» (**pbD**): Alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen (z. B. Namen und Aliase, User-ID, E-Mail, Standortdaten, Anschrift, IMEI, Security Identifier (SID) unter Windows, IP-Adressen, Matrikelnummer, bestimmte Protokolldaten).[1]

«Besondere Kategorie pbD»: pbD, aus denen u.a. die rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen hervorgehen, sowie genetische Daten, biometrische Daten zur eindeutigen Identifizierung einer natürlichen Person, Gesundheitsdaten oder Daten zum Sexualleben oder der sexuellen Orientierung.[2]

«**Verarbeitung**»: jedweder Vorgang i.Z.m. pbD (z. B. Erheben, Ordnen, Verändern, Abfragen, Speichern, Verwenden, Offenlegen, Verbreiten, Abgleichen oder Verknüpfen, Löschen).[3]

«**Verantwortliche**»: Jene Stelle, die über die Zwecke und Mittel der Verarbeitung von pbD entscheidet.[4]

«**Auftragsverarbeiter(in)**» (**AV**): Jene Stelle, die pbD im Auftrag der oder des Verantwortlichen verarbeitet.[5]

Die DSGVO ist bei der Verarbeitung pbD anwendbar.[6] Pseudonymisierte Daten sind pbD.[7] Anonymisierte Daten sind keine pbD.[8] Das Anonymisieren pbD ist eine Datenverarbeitung im Sinne der DSGVO.

Grundsätze

Grundsätze der Verarbeitung:[9]

1. **Rechtmässigkeit** (z. B. Einwilligung, Vertrag, rechtliche Verpflichtung, berechtigtes Interesse), Verarbeitung nach **Treu und Glauben**, **Transparenz** (in für die betr. Pers. nachvollziehbarer Weise);
2. **Zweckbindung** (Verarbeitung nur für festgelegte, eindeutige und legitime Zwecke, pbD dürfen grds. nicht zu anderen Zwecken weiterverarbeitet werden);
3. **Datenminimierung** (Verarbeitungen pbD sind dem Zweck angemessen und auf das erforderliche Mass beschränkt);
4. **Richtigkeit** (pbD sind sachlich richtig und erforderlichenfalls auf dem neuesten Stand);
5. **Speicherbegrenzung** (die Verarbeitung von pbD erfolgt nur so lange, wie es für die Zwecke erforderlich ist);
6. **Integrität** und **Vertraulichkeit** (z. B. Datensicherheit durch geeignete TOMs);
7. **Rechenschaftspflicht** (z. B. Dokumentation und Protokollierung der Verarbeitung).

Technische Systeme müssen so ausgestaltet sein und betrieben werden, dass den zuvor erwähnten Grundsätzen entsprochen wird.[10]

Bei Verarbeitung pbD werden stets die damit verbundenen **Risiken für die Rechte und Freiheiten natürlicher Personen** betrachtet.[11]

Dokumentation

Es existiert ein **schriftliches Verzeichnis** aller Verarbeitungstätigkeiten.[12] Dieses Verzeichnis enthält u.a. folgende Angaben:[13]

- Zwecke der Verarbeitung;
- Beschreibung der Kategorien betr. Pers. und der Kategorien pbD;
- Kategorien von Empfängern, gegenüber denen die pbD offengelegt worden sind oder noch offengelegt werden;
- Angaben zu Übermittlungen in ein Drittland (ggf. Dokumentation geeigneter Garantien);
- Dauer, für die die pbD gespeichert werden oder – falls nicht möglich – die Kriterien für die Festlegung dieser Dauer;[14]
- Allgemeine Beschreibung der TOMs;
- Quelle der pbD (ggf. ob sie aus öffentlich zugänglichen Quellen stammen).[15]

Im Falle einer automatisierten Entscheidungsfindung einschliesslich Profiling[16] existieren aussagekräftige Informationen über die involvierte Logik sowie die Tragweite und die angestrebten Auswirkungen einer derartigen Verarbeitung für die betr. Pers.[17]

Protokollierung

Bei der Verarbeitung von besonderen Kategorien pbD sind TOMs zu implementieren, die gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem pbD eingegeben, verändert oder entfernt worden sind.[18]

Zum Nachweis der Einhaltung der DSGVO ist die Datenverarbeitung angemessen zu protokollieren.[19] Protokolldaten sind in der Regel ebenfalls pbD und entsprechend zu schützen.

Lebenszyklus pbD

pbD erheben: Es werden nur jene pbD Daten erhoben, die für den jeweiligen Zweck angemessen und notwendig sind.[20]

pbD verarbeiten: Jede Verarbeitung pbD erfolgt zu eindeutig festgelegten und legitimen Zwecken.[21]

Jede Verarbeitung pbD ist für den Zweck angemessen und auf das notwendige Mass beschränkt (Datenminimierung).[22]

Angemessene Massnahmen sind zu treffen, damit pbD, die im Hinblick auf die Zwecke ihrer Verarbeitung unrichtig sind, unverzüglich berichtigt werden.[23]

Die Verarbeitung pbD für andere Zwecke als den, für den sie erhoben wurden, ist nur unter bestimmten Voraussetzungen zulässig.[24]

pbD speichern: Das «blosse» Speichern pbD stellt bereits eine Datenverarbeitung dar.[25]

pbD übermitteln: Jede Übermittlung (Datentransfer) pbD erfolgt über sichere Kommunikationskanäle.[26]

Jedwede **Übermittlung pbD an ein Drittland** (an einen nicht EWR/EU-Mitgliedsstaat) ist nur unter bestimmten Bedingungen zulässig. Diese Bedingungen gelten ebenso bei etwaiger Weiterübermittlung aus dem betreffenden Drittland an ein anderes Drittland.[27]

So ist eine Übermittlung pbD in ein Drittland u.a. zulässig, wenn ein angemessenes Datenschutzniveau besteht.[28]

Drittländer mit **angemessenem Datenschutzniveau** sind dzt.: Andorra; Argentinien; Färöer; Guernsey; Insel Man; Israel; Japan; Jersey; Kanada; Neuseeland; **Schweiz** und Uruguay.[29] Eine Übermittlungen pbD in diese Drittländer bedarf keiner besonderen Genehmigung.[30]

pbD löschen: Die Verarbeitung pbD ist so ausgestaltet, dass pbD gelöscht werden können.[31] Die pbD sind u.a. unverzüglich zu löschen, wenn[32]

- sie für die Zwecke, für die sie erhoben oder auf sonstige Weise verarbeitet wurden, nicht mehr notwendig sind;
- die pbD unrechtmässig verarbeitet werden;
- die Löschung der pbD zur Erfüllung einer rechtlichen Verpflichtung erforderlich ist;
- die betr. Pers. ihre Einwilligung widerruft oder Widerspruch gegen die Verarbeitung einlegt.

Es gibt jedoch Ausnahmen betreffend die erwähnte Löschverpflichtung.[33]

Allen Empfängern, denen die pbD offengelegt wurden, ist die Löschung der pbD Daten mitzuteilen.[34]

Datensicherheit

Für jede Verarbeitung pbD ist ein dem Risiko angemessenes **Schutzniveau** festzulegen.[35]

Die TOMs müssen geeignet sein, um das festgelegte Schutzniveau zu gewährleisten.[36]

Die geeigneten TOMs berücksichtigen[37]

- den Stand der Technik,
- die Implementierungskosten und
- die Art, den Umfang, die Umstände und die Zwecke der Verarbeitung sowie

Städtle 38 | Postfach 684 | 9490 Vaduz | Liechtenstein | T +423 236 60 90 | info.dss@llv.li | www.datenschutzstelle.li

- die mit der Verarbeitung verbundenen Risiken für die Rechte und Freiheiten natürlicher Personen.

Mit dem **Standard-Datenschutzmodell (SDM)** existiert ein Werkzeug, das bei der **risikoadäquaten Auswahl** und bei der **Umsetzung rechtlicher Anforderungen in konkrete TOMs** unterstützt.[38]

Die TOMs können je nach Situation u.a. Folgendes umfassen:[39]

- Pseudonymisierung und Verschlüsselung;
- Fähigkeit,
  - die Vertraulichkeit,
  - die Integrität,
  - die Verfügbarkeit und
  - die Belastbarkeit

  der **Systeme und Dienste** i.Z.m. mit der Verarbeitung pbD auf Dauer sicherzustellen;
- Fähigkeit, die **Verfügbarkeit** der pbD und den Zugang zu ihnen bei einem physischen oder technischen **Zwischenfall rasch wiederherzustellen**;
- Verfahren zur regelmässigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der TOMs zur Gewährleistung der Sicherheit der Verarbeitung.[40]

Aus der DSGVO lassen sich insb. die folgenden datenschutzrechtlichen Anforderungen («**Gewährleistungsziele**») an die Datensicherheit ableiten: Vertraulichkeit, Integrität, Verfügbarkeit, Datenminimierung, Nichtverkettung, Transparenz, Intervenierbarkeit, Belastbarkeit und Wiederherstellbarkeit.[41]

Typische Massnahmen zur Gewährleistung der **Vertraulichkeit** sind z. B.: Festlegung eines Berechtigungs- und Rollenkonzeptes, Implementierung eines sicheren Authentifizierungsverfahrens, Verschlüsselung von gespeicherten oder transferierten pbD, Einsatz kryptografischer Verfahren zum Schutz pbD.

Typische Massnahmen zur Gewährleistung der **Integrität** sind z. B.: Einschränkung von Schreib- und Änderungsrechten, Einsatz von Prüfsummen, elektronische Signaturen, dokumentierte Zuweisung von Berechtigungen und Rollen.

Typische Massnahmen zur Gewährleistung der **Verfügbarkeit** sind z. B.: Sicherungskopien (Backups), Redundanz von Hard- und Software.

Typische Massnahmen zur Gewährleistung der **Datenminimierung** sind z. B.: Reduzierung von erfassten Attributen der betr. Pers., Implementierung von Datenmasken, die bestimmte Datenfelder unterdrücken.

Typische Massnahmen zur Gewährleistung der **Nichtverkettung** (Zweckbindung) sind z. B.: Einsatz von zweckspezifischen oder bereichsspezifischen Pseudonymen, geregelte Zweckänderungsverfahren.

Typische Massnahmen zur Gewährleistung der **Transparenz** sind z. B.: Versionierung, Protokollierung, Dokumentation der Verträge mit den internen Mitarbeitenden und mit externen Dienstleistern, Geschäftsverteilungspläne und Zuständigkeitsregelungen.

Typische Massnahmen zur Gewährleistung der **Intervenierbarkeit** sind z. B.: Schaffung notwendiger Datenfelder z. B. für Sperrkennzeichnungen, Benachrichtigungen, Einwilligungen, Widersprüche oder die Deaktivierungsmöglichkeit einzelner Funktionalitäten.

Typische Massnahmen zur Gewährleistung der **Belastbarkeit**[42] sind z. B.: Schutz vor Schadsoftware, Sabotage und höherer Gewalt, Härten von IT-Systemen etwa dadurch, dass nicht benötigte Funktionalitäten – ggf. temporär – deaktiviert werden.

Typische Massnahmen zur Gewährleistung der **Wiederherstellbarkeit**[43] sind z. B.: Umsetzung von Reparaturstrategien und Ausweichprozessen, Erstellung eines Notfallkonzepts zur Wiederherstellung einer Verarbeitungstätigkeit.

Bei der Auswahl der TOMs orientiert sich der Verantwortliche an anerkannten (branchenspezifischen) **Standards**.[44]

Die TOMs sind sowohl zum **Zeitpunkt** der eigentlichen Verarbeitung als auch bereits zum Zeitpunkt der Festlegung der Mittel für die Verarbeitung zu berücksichtigen (*data protection by design and by default*).[45]

Die TOMs sind geeignet, um sicherzustellen *und* den Nachweis dafür zu erbringen, dass die Verarbeitung pbD gem. DSGVO erfolgt.[46]

Bei der Verarbeitung pbD ist zu gewährleisten, dass die Sicherheit der Verarbeitung die Einrichtung eines Verfahrens zur **regelmässigen Überprüfung**, Bewertung und Evaluierung der Wirksamkeit der TOMs umfasst.[47]

Voreinstellungen

Mit geeigneten TOMs ist sicherzustellen, dass durch **Voreinstellungen** grds. nur pbD, deren Verarbeitung für den jeweiligen bestimmten Verarbeitungszweck erforderlich ist, verarbeitet werden.[48]

Diese Verpflichtung gilt für die Gesamtheit der erhobenen pbD, den Umfang ihrer Verarbeitung, ihre Speicherfrist und ihre Zugänglichkeit.[49]

Datenschutzverletzungen

«Verletzung des Schutzes pbD» ist eine Verletzung der Sicherheit, die zur Vernichtung, zum Verlust oder zur Veränderung, ob unbeabsichtigt oder unrechtmässig, oder zur unbefugten Offenlegung von bzw. zum unbefugten Zugang zu pbD führt, die übermittelt, gespeichert oder auf sonstige Weise verarbeitet wurden.[50]

Eine Verletzung des Schutzes pbD ist durch den AV unverzüglich dem Verantwortlichen zu melden. Dieser prüft eine etwaige **Meldepflicht** an die DSS. Besteht ein Risiko für die Rechte und Freiheiten natürlicher Personen, so ist die Verletzung durch den Verantwortlichen binnen 72 Stunden ab Kenntnis der DSS zu melden. Ist dieses Risiko als hoch einzustufen, sind zusätzlich die betr. Pers. unverzüglich zu benachrichtigen.[51]

Eine Meldung an den Verantwortlichen und die DSS enthält u.a. folgende Informationen:[52]

- Beschreibung der Art der Verletzung des Schutzes pbD, soweit möglich mit Angabe der Kategorien und der ungefähren Zahl der betr. Pers., der betroffenen Kategorien und der ungefähren Zahl der Datensätze;
- Beschreibung der ergriffenen oder vorgeschlagenen Massnahmen zur Behebung der Verletzung des Schutzes pbD und ggf. Massnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen.

Sofern die **Informationen** nicht unmittelbar bereitgestellt werden können, können diese ohne unangemessene weitere Verzögerung **schrittweise** zur Verfügung gestellt werden.[53]

Verletzungen des Schutzes pbD, einschliesslich aller i.Z.m. der Verletzung des Schutzes pbD stehenden Fakten, ihrer Auswirkungen und der ergriffenen Abhilfemassnahmen sind – ungeachtet einer Meldung an die DSS – zu **dokumentieren**.[54]

Datenschutz-Folgenabschätzung (DSFA)

Hat eine Form der Verarbeitung pbD, insb. bei Verwendung neuer Technologien, aufgrund der Art, des Umfangs, der Umstände und der Zwecke der **Verarbeitung voraussichtlich** ein **hohes Risiko** für die Rechte und Freiheiten natürlicher Personen (Schwellwertanalyse) zur Folge, so ist **vorab eine Abschätzung der Folgen** der vorgesehenen Verarbeitungsvorgänge für den Schutz pbD durchzuführen.[55]

Die DSFA enthält zumindest Folgendes:[56]

- systematische **Beschreibung** der geplanten Verarbeitungsvorgänge und der Zwecke der Verarbeitung, ggf. einschliesslich der von dem Verantwortlichen verfolgten berechtigten Interessen;
- **Bewertung** der Notwendigkeit und Verhältnismässigkeit **der Verarbeitungsvorgänge** in Bezug auf den Zweck;
- **Bewertung der Risiken** für die Rechte und Freiheiten der betr. Pers.;
- die zur Bewältigung der Risiken geplanten **Abhilfemassnahmen**.

Vor der Verarbeitung pbD ist die **DSS zu konsultieren**, wenn aus einer DSFA hervorgeht, dass die Verarbeitung ein hohes Risiko zur Folge hätte, sofern keine Massnahmen zur Eindämmung des Risikos getroffen werden.[57]

Der DSS sind bei einer Konsultation folgende Informationen zur Verfügung zu stellen:[58]

- ggf. Angaben zu den jeweiligen Zuständigkeiten des Verantwortlichen, der gemeinsam Verantwortlichen und der an der Verarbeitung beteiligten AVs;
- Zwecke und die Mittel der beabsichtigten Verarbeitung;
- die zum Schutz der Rechte und Freiheiten der betr. Pers. gem. DSGVO vorgesehenen Massnahmen und Garantien;
- die DSFA;
- alle sonstigen von der DSS angeforderten Informationen.

Erforderlichenfalls ist durch den Verantwortlichen eine **Überprüfung** durchzuführen, um zu bewerten, ob die **Verarbeitung pbD gem. der DSFA durchgeführt wird**; dies gilt zumindest, wenn hinsichtlich des mit den Verarbeitungsvorgängen verbundenen Risikos Änderungen eingetreten sind.[59]

Auftragsverarbeitung

Eine **Zusammenarbeit** ist nur mit AVs zulässig, die hinreichend Garantien dafür bieten, dass geeignete TOMs im Einsatz sind, sodass die Verarbeitung pbD im Einklang mit den Anforderungen der DSGVO erfolgt und der Schutz der Rechte der betr. Pers. gewährleistet ist.[60]

Ohne vorherige gesonderte oder allgemeine schriftliche Genehmigung ist die Inanspruchnahme von **Unterauftragsverarbeitern** nicht zulässig.[61] Im Fall einer allgemeinen schriftlichen Genehmigung informiert der AV immer über jede beabsichtigte Änderung in Bezug auf die Hinzuziehung oder die Ersetzung anderer AVs.[62]

Die Verarbeitung pbD durch einen AV erfolgt auf der Grundlage eines **schriftlichen Vertrags**.[63] Inhalt des Vertrags ist insb.:[64]

- die Gewährleistung, dass sich die zur Verarbeitung der pbD befugten Personen zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen;
- der Einsatz erforderlicher TOMs;
- ggf. den Verantwortlichen mit TOMs dabei zu unterstützen, der Pflicht zur Wahrnehmung der Rechte der betr. Pers. nachzukommen;
- Unterstützung des Verantwortlichen bei der Einhaltung der in den Art. 32 bis 36 DSGVO genannten Pflichten;
- dass nach der Erbringung der Verarbeitungsleistungen alle pbD entweder gelöscht oder an den Verantwortlichen zurückgegeben und die vorhandenen Kopien gelöscht werden;
- Zurverfügungstellung aller erforderlichen Informationen zum Nachweis der Einhaltung der DSGVO;
- Überprüfungen – einschliesslich Inspektionen – zu ermöglichen und dazu beizutragen.

Rechte betroffener Personen

Die Verarbeitung pbD ist so ausgestaltet, dass den Rechten der betr. Pers. entsprochen werden kann. Eine betr. Pers. kann gem. DSGVO gegenüber dem Verantwortlichen die folgenden Rechte geltend machen:[65]

- auf Information;[66]
- auf Auskunft;[67]
- auf Berichtigung;[68]
- auf Löschung;[69]
- auf Einschränkung der Verarbeitung;[70]
- auf Datenübertragbarkeit;[71]
- auf Widerspruch;[72]
- auf Widerruf; [73]
- nicht einer ausschliesslich auf einer automatisierten Verarbeitung beruhenden Entscheidung unterworfen zu werden, die ihr gegenüber rechtliche Wirkung entfaltet.[74]

Mit entsprechenden TOMs wird der Verantwortliche dabei unterstützt, seiner Pflicht auf Wahrnehmung der zuvor genannten Rechte der betr. Pers. nachzukommen.[75]

Informationen i.Z.m. der Verarbeitung der pbD werden den betr. Pers. in präziser, transparenter, verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache zur Verfügung gestellt.[76]

Auskunft: Die Verarbeitung pbD ist so ausgestaltet, dass der betr. Pers. auf Antrag[77] Informationen unverzüglich, jedenfalls jedoch innerhalb eines Monats nach Eingang des Antrags zugehen.[78]

Der betr. Pers. wird **auf Antrag eine Kopie** ihrer pbD, die Gegenstand der Verarbeitung sind, zur Verfügung gestellt.[79]

Bestehen begründete Zweifel an der Identität einer natürlichen Person, können zusätzliche Informationen angefordert werden, die zur Bestätigung der Identität der betr. Pers. erforderlich sind.[80]

Berichtigung: Unrichtige pbD sind auf Verlangen der betr. Pers. unverzüglich zu berichtigen.[81]

Jede betr. Pers. kann – unter Berücksichtigung der Zwecke der Verarbeitung – die Vervollständigung unvollständiger pbD verlangen.[82]

Allen Empfängern, denen die pbD offengelegt wurden, ist die Berichtigung der pbD Daten mitzuteilen.[83]

Löschung: Die betr. Pers. kann unter bestimmten Voraussetzungen verlangen, dass sie betreffende pbD unverzüglich gelöscht werden.[84]

Hat der Verantwortliche die pbD öffentlich gemacht und ist er zu deren Löschung verpflichtet, so trifft er angemessene Massnahmen, um andere Verantwortliche die die pbD verarbeiten, darüber zu informieren, dass eine betr. Pers. die Löschung verlangt hat.[85]

Einschränkung: Die Verarbeitung pbD ist so ausgestaltet, dass sie eingeschränkt werden kann, wenn eine der folgenden Voraussetzungen gegeben ist:[86]

- die Richtigkeit der pbD wird von der betr. Pers. bestritten;
- die Verarbeitung ist unrechtmässig und die betr. Pers. lehnt die Löschung der pbD ab;
- die pbD werden für die Zwecke der Verarbeitung nicht länger benötigt, die betr. Pers. benötigt sie jedoch zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen;
- die betr. Pers. hat Widerspruch gegen die Verarbeitung eingelegt hat, solange noch nicht feststeht, ob die berechtigten Gründe des Verantwortlichen gegenüber denen der betr. Pers. überwiegen.

Wurde die Verarbeitung eingeschränkt, so dürfen die pbD – von ihrer Speicherung abgesehen – nur begründet (z. B. Einwilligung der betr. Pers. oder zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen) verarbeitet werden.[87]

Allen Empfängern, denen die pbD offengelegt wurden, ist die Einschränkung der Verarbeitung der pbD mitzuteilen.[88]

Datenübertragbarkeit: Die Verarbeitung pbD ist so ausgestaltet, dass betr. Pers., die sie betreffenden pbD, die sie selbst bereitgestellt haben, in einem strukturierten, gängigen und maschinenlesbaren Format übermittelt werden können.[89]

Die betr. Pers. kann in bestimmten Fällen verlangen, dass die sie betreffenden pbD direkt von einem Verantwortlichen einem anderen Verantwortlichen übermittelt werden, soweit dies technisch machbar ist.[90]

Widerspruch: Eine betr. Pers. kann in gewissen Fällen gegen die Verarbeitung sie betreffender pbD Widerspruch einlegen.[91] Eine Verarbeitung der pbD ist danach nicht mehr zulässig, es sei denn, es können zwingende schutzwürdige Gründe für die Verarbeitung nachgewiesen werden.[92]

Widerruf: Eine betr. Pers. kann ihre Einwilligung in eine Verarbeitung jederzeit widerrufen. Eine Verarbeitung, die auf Einwilligungen basiert, ist so auszugestalten, dass dies ab dem Widerruf berücksichtigt werden kann.[93]

Datenschutzbeauftragter (DSB)

Wurde ein DSB benannt, darf dieser wegen der geforderten Unabhängigkeit innerhalb des Unternehmens keine Tätigkeit ausüben, welche zur Entscheidung über Zwecke und Mittel einer Verarbeitung von pbD führt. Positionen die zu einem Interessenkonflikt führen sind z. B. der Leiter der IT oder ein Geschäftsleitungsmitglied.[94]

Videoüberwachung

Die Beobachtung **öffentlich zugänglicher Räume** mit optisch-elektronischen Einrichtungen (Videoüberwachung) ist grds. vor der Inbetriebnahme der DSS zu melden.[95] Von einer Meldung ausgenommen sind Bildübermittlungen in Echtzeit ohne Aufzeichnungs- oder sonstige weitere Verarbeitungsmöglichkeit.

Nicht öffentlich sind: Büro- und Serverräume, Rechenzentren, Werkshallen bzw. allgemein Arbeitsplätze, zu denen nur die Betriebsangehörigen und berechtigte Mitarbeitende mittels eines Schlüssels oder PIN-Codes Zutritt haben.[96]

Bei der Auswahl eines Videoüberwachungssystems sind insb. die technischen und organisatorischen Aspekte zu berücksichtigen. So sind etwa bei der Implementierung konkreter TOMs (Datensicherheit) vor allem die Art, der Umfang sowie die Umstände und Zwecke der Videoüberwachung zu berücksichtigen.

Je nach Nutzung und Zweck der Videoüberwachung ist das **Ausschwärzen oder Verpixeln** vom Fokus erfasster Bereiche notwendig.

Jedenfalls muss der Zugriff auf die Videoaufnahmen geschützt und auf eine beschränkte Anzahl von Personen eingeschränkt sein.[97]

Technik und Geldbussen

Verstösse gegen Bestimmungen der DSGVO zu Pflichten i.Z.m. der Datensicherheit können mit Geldbussen geahndet werden.[98]

Bei der Entscheidung der DSS über die Verhängung einer Geldbusse und über deren Betrag wird in jedem Einzelfall u.a. Folgendes gebührend berücksichtigt:[99]

- jegliche getroffenen Massnahmen zur Minderung des den betr. Pers. entstandenen Schadens;
- Grad der Verantwortung unter Berücksichtigung der gem. den Art. 25 und 32 DSGVO getroffenen TOMs.

Abkürzungsverzeichnis	
Abs.	Absatz
Art.	Artikel
AV	Auftragsverarbeiter(in)
betr. Pers.	betroffene Person / betroffene Personen[100]
Bst.	Buchstabe
DSB	Datenschutzbeauftragte(r)
DSFA	Datenschutz-Folgenabschätzung
DSGVO	Datenschutz-Grundverordnung
DSS	Datenschutzstelle (www.datenschutzstelle.li)
dzt.	derzeit
gem.	gemäss
ggf.	gegebenenfalls
grds.	grundsätzlich
i.V.m.	in Verbindung mit
i.Z.m.	im Zusammenhang mit
insb.	insbesondere
pbD	personenbezogene Daten
SDM	Standard-Datenschutzmodell
TOMs	technische und organisatorische Massnahmen
u.a.	unter anderem
vgl.	vergleiche
z. B.	zum Beispiel
Ziff.	Ziffer

[1] Art. 4 Ziff. 1 DSGVO.
[2] Art. 9 Abs. 1 DSGVO.
[3] Art. 4 Ziff. 2 DSGVO.
[4] Art. 4 Ziff. 7 DSGVO.
[5] Art. 4 Ziff. 8 DSGVO.
[6] Siehe sachlicher (Art. 2 DSGVO) und räumlicher (Art. 3 DSGVO) Anwendungsbereich sowie https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_3_2018_territorial_scope_after_consultation_de.pdf.
[7] Vgl. Art. 4 Ziff. 5 DSGVO.
[8] ErwGr. 26 DSGVO sowie https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_de.pdf.
[9] Siehe https://www.datenschutzstelle.li/datenschutz/themen-z/grundsaetze-fuer-die-verarbeitung-personenbezogener-daten-art-5-dsgvo.
[10] Art. 25 Abs. 1 DSGVO, https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-42019-article-25-data-protection-design-and_en.
[11] Vgl. unter anderem Art. 24, 25, 32 bis 35 DSGVO.
[12] Art. 30 DSGVO, https://www.datenschutzstelle.li/datenschutz/themen-z/verzeichnis-verarbeitungstaetigkeiten.
[13] Art. 30 Abs. 1 DSGVO.
[14] Vgl. Art. 13 Abs. 2 Bst. a DSGVO.
[15] Vgl. Art. 14 Abs. 2 Bst. f DSGVO.
[16] Art. 4 Ziff. 4 DSGVO.
[17] Art. 15 Abs. 1 Bst. h DSGVO.
[18] Vgl. Art. 21 Abs. 2 Bst. b DSG.
[19] Art. 5 Abs. 2 DSGVO (Grundsatz), Art. 7 Abs. 1 DSGVO (Einwilligung), Art. 24 Abs. 1 DSGVO (Verantwortung des Verantwortlichen), Art. 28 Abs. 3 Bst. h DSGVO (Auftragsverarbeitung), Art. 35 DSGVO (DSFA).
[20] Art. 5 Abs. 1 Bst. c DSGVO.
[21] Vgl. Art. 5 Abs. 1 Bst. b und c DSGVO.
[22] Art. 5 Abs. 1 Bst. c DSGVO.
[23] Art. 5 Abs. 1 Bst. d DSGVO.
[24] Informationspflicht gemäss Art. 13 Abs. 3 DSGVO und Voraussetzungen gemäss Art. 22 und 23 DSG.
[25] Vgl. Art. 4 Ziff. 2 DSGVO.
[26] Vgl. Art. 25 und 32 Abs. 1 Bst. a DSGVO.
[27] Art. 44 Abs. 1 DSGVO.
[28] Art. 45 Abs. 1 DSGVO.
[29] Anhang 1 Datenschutzverordnung.
[30] Art. 45 Abs. 1 DSGVO iVm Anhang 1 DSV.
[31] Art. 5 Abs. 1 Bst. e DSGVO.
[32] Art. 17 Abs. 1 DSGVO.
[33] Art. 17 Abs. 3 DSGVO.
[34] Art. 19 DSGVO.
[35] Art. 32 Abs. 2 DSGVO.
[36] Art. 32 Abs. 1 DSGVO.
[37] Art. 25 Abs. 1 DSGVO.
[38] https://www.datenschutz-mv.de/datenschutz/datenschutzmodell/ und https://www.datenschutz-mv.de/static/DS/Dateien/Datenschutzmodell/SDM-Methode_V20b.pdf.
[39] Art. 32 Abs. 1 DSGVO.
[40] Art. 32 Abs. 1 Bst. d sowie Art. 24 Abs. 1 DSGVO.
[41] SDM, Abschnitt C1, Seite 25 ff.
[42] Art. 32 Abs. 1 Bst. b DSGVO.
[43] Art. 32 Abs. 1 Bst. c DSGVO.
[44] Vgl. Stand der Technik, Art. 25 Abs. 1 und Art. 32 Abs. 1 DSGVO.
[45] Art. 25 Abs. 1 DSGVO.
[46] Art. 24 Abs. 1 DSGVO.
[47] Art. 32 Abs. 1 Bst. d DSGVO und Art. 21 Abs. 2 Bst. i DSG.
[48] Art. 25 Abs. 2 DSGVO.
[49] Art. 25 Abs. 2 DSGVO.
[50] Art. 4 Ziff. 12 DSGVO, https://www.datenschutzstelle.li/datenschutz/themen-z/meldung-von-datenschutzverletzungen-art-33-dsgvo.
[51] Art. 33 Abs. 1 und 2 sowie Art. 34 Abs. 1 DSGVO.
[52] Art. 33 Abs. 3 DSGVO, Meldeformular: https://www.datenschutzstelle.li/services-und-downloads/formulare#MeldungDatenschutzVerletzung.
[53] Art. 33 Abs. 4 DSGVO.
[54] Art. 33 Abs. 5 DSGVO.
[55] Art. 35 DSGVO, https://www.datenschutzstelle.li/datenschutz/themen-z/datenschutz-folgenabschaetzung, https://www.datenschutzstelle.li/download_file/542/315.
[56] Art. 35 Abs. 7 DSGVO.
[57] Art. 36 Abs. 1 DSGVO.
[58] Art. 36 Abs. 3 DSGVO.
[59] Art. 35 Abs. 11 DSGVO.
[60] Art. 28 Abs. 1 DSGVO.
[61] Art. 28 Abs. 2 DSGVO.
[62] Art. 28 Abs. 2 DSGVO.
[63] Art. 28 Abs. 3 iVm Art. 28 Abs. 9 DSGVO.
[64] Art. 28 Abs. 3 DSGVO.
[65] Kapitel III (Art. 12 bis 23) DSGVO.
[66] Art. 13 und 14 DSGVO.
[67] Art. 15 DSGVO.
[68] Art. 16 DSGVO.
[69] Art. 17 DSGVO.
[70] Art. 18 DSGVO.
[71] Art. 20 DSGVO.
[72] Art. 21 DSGVO.
[73] Art. 7 DSGVO.
[74] Art. 22 DSGVO.
[75] Vgl. Art. 28 Abs. 3 Bst. e DSGVO.
[76] Art. 12 Abs. 1, Art. 13, Art. 14 DSGVO.
[77] Gemäss Art. 15 bis 22 DSGVO (Rechte der betroffenen Personen).
[78] Art. 12 Abs. 3 DSGVO.
[79] Art. 15 Abs. 3 DSGVO.
[80] Vgl. Art. 12 Abs. 6 DSGVO.
[81] Art. 16 DSGVO, ErwGr. 59.
[82] Art. 16 DSGVO.
[83] Art. 19 DSGVO.
[84] Art. 17 Abs. 1 DSGVO.
[85] Art. 17 Abs. 2 DSGVO.
[86] Art. 18 Abs. 1 DSGVO.
[87] Art. 18 Abs. 2 DSGVO.
[88] Art. 19 DSGVO.
[89] Art. 20 Abs. 1 DSGVO, https://www.datenschutzstelle.li/application/files/9215/3622/8391/wp242rev01_de.pdf.
[90] Art. 20 Abs. 2 DSGVO.
[91] Art. 21 Abs. 1 i.V.m. Art. 6 Abs. 1 Bst. e oder f DSGVO.
[92] Art. 21 Abs. 1 DSGVO.
[93] Art. 7 Abs. 3 DSGVO.
[94] Leitlinien in Bezug auf Datenschutzbeauftragte („DSB“), WP 243 rev.01, Abschnitt 3.5, Seite 19, https://www.datenschutzstelle.li/application/files/5715/3622/9517/wp243rev01_de.pdf.
[95] Art. 5 Abs. 7 DSG.
[96] https://www.datenschutzstelle.li/datenschutz/themen-z/videoueberwachung-fuer-betreiber.
[97] https://www.datenschutzstelle.li/datenschutz/themen-z/videoueberwachung-fuer-betreiber.
[98] Art. 83 Abs. 4 DSGVO.
[99] Art. 83 Abs. 2 DSGVO.
[100] Vgl. Art. 4 Ziff. 1 DSGVO.