BASEL LANDSCHAFT
AUFSICHTSSTELLE DATENSCHUTZ

Erläuterungen und Beispiele Schutzbedarfsanalyse

Version: V 1.9 vom 15.8.2024

Das vorliegende Dokument richtet sich primär an Behörden der kantonalen Verwaltung, da es an zusätzliche dort geltende Regelwerke und konzeptionellen Grundlagen zur Informationssicherheit anknüpft.

Für Gemeinden, öffentlich rechtliche Körperschaften und Anstalten sowie Private, die eine öffentliche Aufgabe erfüllen, kann es sinngemäss verwendet werden.

BASEL LANDSCHAFT

Inhaltsverzeichnis

0. Zweck des Dokumentes

Diese Hilfestellung richtet sich an Informationseigner[1] als Verantwortliche für die bearbeiteten Informationen sowie an IT-Sicherheitsbeauftragte und Informatik-Projektleitende, welche beim sicheren Umgang mit Informationen unterstützen.

1. Ausgangslage

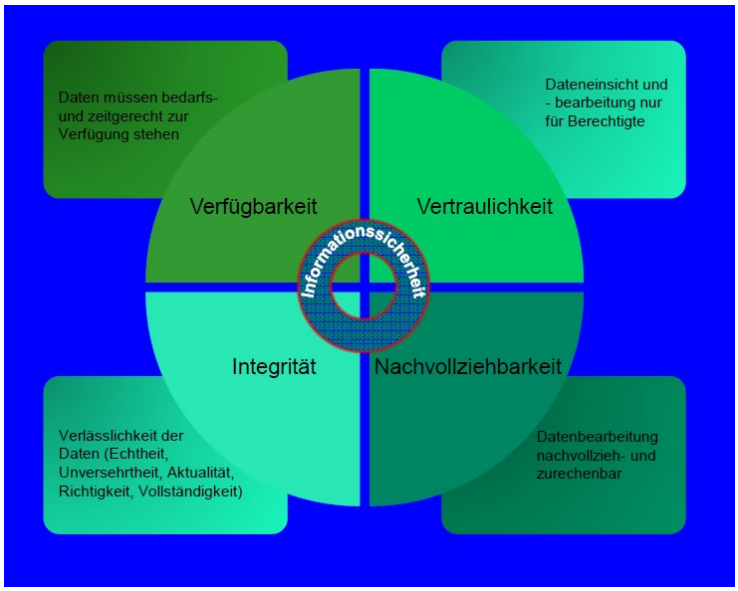
In § 8 Abs. 1 des Gesetzes über die Informationen und den Datenschutz (Informations- und Datenschutzgesetz, IDG, SGS 162) wird festgelegt, dass Informationen von der Informationseignerin mit Hilfe von angemessen organisatorischen und technischen Massnahmen vor Verlust, Entwendung sowie unrechtmässiger Bearbeitung und Kenntnisnahme geschützt werden müssen. Der Schutzbedarf der Informationsbestände ergibt sich aus einer ersten groben Einstufung zu den einzelnen Schutzzielen. Auf dieser Basis werden die weiteren Massnahmen zum Schutz der Informationen geplant und umgesetzt.

§ 2 Abs. 2 der Verordnung zum Gesetz über die Information und den Datenschutz (Informations- und Datenschutzverordnung, IDV, SGS 162.11) hält fest, dass die Schutzziele Vertraulichkeit, Verfügbarkeit und Richtigkeit der Daten (Integrität) berücksichtigt werden müssen. Zusätzlich muss in der öffentlichen Verwaltung des Kantons Basel-Landschaft das Schutzziel Nachvollziehbarkeit berücksichtigt werden (§ 4 Abs. 1 des Gesetzes über die Archivierung (Archivgesetz; SGS 163)). § 5 der Verordnung über die Informationssicherheit (VIS; SGS 162.51) regelt, dass Informationen entsprechend ihrem Schutzbedarf anhand eines Rasters klassifiziert werden.

Auf diesen gesetzlichen Grundlagen fussen die Erläuterungen und Beispiele. Dabei gilt es zu bedenken, dass auch der Schutzbedarf von Informationen, oder Prozessen ohne Personenbezug analysiert werden muss (bspw. Finanzdaten).

2. Schutzbedarf

In der öffentlichen Verwaltung des Kantons Basel-Landschaft werden Projekte anhand der Projektmanagementmethode HERMES realisiert. Mit der Schutzbedarfsanalyse klassifiziert der Informationseigner die Informationsbestände und legt damit den Grundstein für die Anforderungen an die Informationssicherheit und den Datenschutz.



Betrachtet werden dabei die Schutzziele Vertraulichkeit, Verfügbarkeit, Integrität und Nachvollziehbarkeit.

[1] Öffentliches Organ, das die Informationen zur Erfüllung seiner gesetzlichen Aufgaben bearbeitet

Die Analyse des Schutzbedarfs gestaltet sich für Informationseigner und Projektbeteiligte nicht immer ganz einfach. Oft stellen sich schon zu Beginn grundsätzliche Fragen zu den Informationen. Typische Fragen, die bei dieser Analyse beantwortet werden müssen, sind beispielsweise:

- Haben diese Informationen einen Personenbezug und sind deshalb Personendaten?
- Handelt es sich um besondere Personendaten?
- Müssen diese Informationen rund um die Uhr abrufbar sein oder muss dies nur während der normalen Bürozeiten möglich sein?
- Welche Auswirkungen haben falsche Informationen auf die betroffenen Personen, auf die Behörde?

Dieses Dokument soll anhand von Beispielen unterstützen und die Klassifikation der Informationen unter Berücksichtigung der einzelnen Schutzziele vereinfachen. Der dezentrale IT-Sicherheitsbeauftragte (DIT-SIBE) ist mit der Methode der Schutzbedarfsanalyse vertraut und kann als Ansprechperson bei Fragen beigezogen werden.

Die Ergebnisse der Schutzbedarfsanalyse fliessen im Projektablauf in die Risikobeurteilung und die Konzeption der Sicherheitsmassnahmen (ISDS-Konzept) ein. Sie bilden zudem eine Basis für die Entscheidung, ob eine Bearbeitung von Personendaten der gesetzlich vorgeschriebenen Vorabkonsultation unterliegt.

3. Informationen

Als Informationen werden «alle Aufzeichnungen, welche die Erfüllung einer öffentlichen Aufgabe betreffen, unabhängig von ihrer Darstellungsform und ihrem Informationsträger» bezeichnet (§ 3 Abs. 2 IDG).

Personendaten sind nach der gesetzlichen Definition alle Informationen, die sich auf eine bestimmte oder bestimmbare natürliche Person beziehen (§ 3 Abs. 3 IDG). Bestimmt ist eine Person, wenn sie sich direkt aufgrund der Daten identifizieren lässt. Bestimmbar ist sie, wenn sie zwar nicht durch die fraglichen Daten allein, jedoch mit Hilfe anderer Informationen identifiziert werden kann. Kann man Informationen nicht mehr einer einzelnen Person zuordnen, so handelt es sich nicht um Personendaten im Sinne des IDG. Aus diesem Grund bleiben pseudonymisierte Daten für diejenigen Stellen, die Zugang zu den Schlüssel der Pseudonymisierung haben, Personendaten.

Beispiele:

- Roger Federer (bestimmte Person)
- Wimbledon Sieger 2012 (bestimmbare Person)
- Männlicher Einwohner von Valbella (keine Personendaten)
- Benutzeridendifikakation wie bspw. U-Nummer (bestimmbare Person für alle, die Zugang zur Zuordung Benutzeridenfifikation zu Mitarbeitenden haben via Outlook oder auf anderem Weg Kenntnis von dieser erlangen)

Das Gesetz unterscheidet zwischen «besondere Personendaten» und «Personendaten». Der Grund dafür liegt in der Tatsache, dass bei der Bearbeitung bestimmter Informationen die Persönlichkeit besonders zu schützen ist, da davon ausgegangen wird, dass die Datenbearbeitung[2] dieser für die betroffene Person gravierende negative Folgen haben können. So können z.B. Angaben zum Gesundheitszustand einer Person stark in die Persönlichkeitsrechte der Betroffenen eingreifen (z.B. stigmatisierende Befunde wie HIV-positiv, Alkoholismus oder psychische Erkrankungen). Es sind aber nicht alle Gesundheitsdaten besonders schützenswert. So ist die Tatsache,

[2] Gemäss § 3 Abs. 5 IDG ist Bearbeiten jeder Umgang mit Informationen wie das Beschaffen, Aufbewahren, Verwenden (also auch Lesen), Verändern, Bekanntgeben oder Vernichten, unabhängig von den angewandten Mitteln und Verfahren

dass jemand eine Brille trägt oder den Schnupfen hat, kaum geeignet, die Persönlichkeit nachhaltig bzw. gravierend zu verletzen. Ebenfalls zu den besonderen Personendaten gehören sog. Persönlichkeitsprofile. Darunter versteht man eine Zusammenstellung von Informationen, anhand derer eine Beurteilung wesentlicher Aspekte der Persönlichkeit einer natürlichen Person möglich ist. So sind z.B. Angaben über Einkommen, Vermögen, Schule und Beruf, Familienverhältnisse, bisherige Wohnorte für sich alleine in der Regel keine besonderen Personendaten. Die Verknüpfung solcher Angaben kann jedoch ein Profil einer Person ergeben, dessen Bearbeitung stark in die Privatsphäre der Person eingreift oder eingreifen kann. Dies ist insbesondere dann der Fall, wenn Daten über eine längere Zeit zusammengetragen werden und ein biographisches Bild einer Person ergeben.

Unter «besondere Personendaten» fallen nach § 3 Abs. 4 IDG Angaben über: religiöse, weltanschauliche, politische oder gewerkschaftliche Ansichten oder Tätigkeiten, die Gesundheit, das Erbgut(genetische Daten), die Intimsphäre oder die ethnische Herkunft, Behinderungen, Massnahmen der sozialen Hilfe, administrative oder strafrechtliche Verfolgungen und Sanktionen sowie mit speziellen technischen Verfahren gewonnene personenbezogene Daten zu den physischen, physiologischen oder verhaltenstypischen Merkmalen einer natürlichen Person, welche die eindeutige Identifizierung dieser Person ermöglichen oder bestätigen (biometrische Daten), Zusammenstellungen von Informationen, die eine Beurteilung wesentlicher Aspekte der Persönlichkeit einer natürlichen Person erlauben (Persönlichkeitsprofil), wobei diese Aufzählung nicht abschliessend ist.

«Persönlichkeitsprofile» i.S.v. § 3 Abs. 4 Bst. b IDG können von «Profiling» i.S.v. § 3 Abs. 7 IDG unterschieden werden:

Persönlichkeitsprofile sind ein *Produkt einer Datensammlung* zu einer Person, das durch die Datenbearbeitung entstehen kann. Profiling ist jede Auswertung von Informationen, um wesentliche persönliche Merkmale zu analysieren oder Entwicklungen vorherzusagenezüglich Arbeitsleistung, wirtschaftliche Lage, Gesundheit, Intimsphäre oder Mobilität. Profiling ist demnach eine *Tätigkeit* mit dem Zweck der Gewinning von zusätzlichen personenbezogenen Informationen, die sich nicht direkt aus den vorhanden Daten ergeben.

4. Klassifikationsmekmale der Schutzziele

4.1. Vertraulichkeit

Bei der Schutzbedarfsanalyse ist immer auch der Kontext zu beachten, in dem Informationen verwendet werden. Die Einstufung der jeweiligen Information kann je nach Kontext, in dem sie verwendet wird, unterschiedlich ausfallen. So ist beispielsweise die Information zu einer Adresse im Regelfall vertraulich. Befindet sich die betroffene Person aber z.B. in einem Zeugenschutzprogramm, ist die Information streng vertraulich und der Schutzbedarf entsprechend erhöht.

Streng vertrauliche Informationen

Streng vertrauliche Personendaten bergen bei ungenügendem Schutz vor unrechtmässiger Datenbearbeitung wie bspw. Einsichtnahme, Bekanntgabe, ein besonders hohes Risiko für die betroffenen Personen. Bei Informationen ohne Personenbezug betreffen die Risiken das öffentliche Organ bzw. den Kanton.

Streng vertrauliche Personendaten sind wegen der besonderen Gefahr der Verletzung von Grundrechten (z.B. Schutz vor Diskriminierung, Stigmatisierung, Gefährdung) besonders stark zu schützen. Bei dieser Art von Informationen sind im Falle eines nicht angemessenen Schutzes die möglichen Folgen eines Missbrauchs (z.B. einer unrechtmässigen Datenbekanntgabe) für die einzelnen betroffenen Personen gravierend. Das Risiko einer Persönlichkeitsverletzung ist anhand der Art

der Informationen zu analysieren. Es gelten hier sehr strenge Vorschriften betr. technische und organisatorische Massnahmen zum Schutz der Informationen und somit auch zur Vergabe von fallbezogenen Zugriffsrechten.

Ebenfalls streng vertraulich werden in der Regel die Informationen klassifiziert, für welche andere spezielle gesetzliche Geheimhaltungspflichten bestehen (Sozialversicherungsgeheimnis, Sozialhilfegeheimnis, Steuergeheimnis, Opferhilfe, Stimmgeheimnis).

*Beispiele streng vertraulicher Informationen **mit*** Personendaten:

- Die bearbeiteten Informationen im Informatiksystem der Steuerverwaltung sind streng vertraulich (kantonales Steuergeheimnis und fallweise besondere Personendaten (Konfession, Gesundheitsdaten)).
- Informationen zu Kriminalfällen, welche die Polizei sammelt und analysiert, um mutmassliche Täterschaft oder verdächtige Personen zu identifizieren und weitere Kriminalität zu verhindern, sind streng vertraulich (Informationen zu strafrechtlichen Verfolgungen und Sanktionen zählen zu den besonderen Personendaten).
- Dokumente im Rahmen von Zivil- und Strafprozessen (Informationen zu administrativen und strafrechtlichen Verfolgungen) zählen zu den besonderen Personendaten.
- Kalendertermine bei der Staatsanwaltschaft mit Angaben zu Zeugen und Beschuldigten (Informationen zu administrativen und strafrechtlichen Verfolgungen zählen zu den besonderen Personendaten, Informationen zu Zeugen beinhalten ein besonders hohes Risiko.)
- Die Tatsache, dass eine Person aufgrund einer sozialen oder wirtschaftlichen Notlage eine Beratung oder Betreuung in Anspruch nimmt (Informationen zu Massnahmen der sozialen Hilfe zählen zu den besonderen Personendaten).
- Angaben einer Person über Vormundschafts- und Fürsorgemassnahmen, etwa betreffend einen fürsorgerischen Freiheitsentzug (Informationen zu administrativen Massnahmen zählen zu den besonderen Personendaten, hier sind oftmals. auch noch Gesundheitsdaten enthalten).
- Das Kantonsspital Liestal fragt medizinische Befunde bei einem Hausarzt an (Gesundheitsdaten zählen zu den besonderen Personendaten).
- Im elektronischen Personaldossier werden Persönlichkeitsprofile (besondere Personendaten) bearbeitet (Angaben zur Bewerbung, Leistungsbeurteilung, Krankheitsmeldungen etc.).
- Rechnung des geschäftlichen (Mobil-)Telefons zur privaten Mitnutzung eines Mitarbeitenden mit sämtlichen Verbindungsdaten. Diese Verbindungsdaten können besondere Personendaten enthalten (Nutzung der betrieblichen Telefone z.B. bei der StaWa, der Polizei; bei privater Nutzung z.B. Anrufe bei Ärzten, Beratungsstellen etc.).
- Die Benutzerkennung und das dazugehörige Passwort (Das Passwort muss persönlich und geheim sein und ist deshalb streng vertraulich).

*Beispiele streng vertraulicher Informationen **ohne*** Personendaten:

- Informationen, welche zwischen Hochbauamt und externen Architekten zu sicherheitsrelevanten Liegenschaften (Bsp. Gefängnis ohne Insassen) ausgetauscht werden.
- Zugangscode zu kritischen Infrastrukturen.

Vertrauliche Informationen

Vertrauliche Informationen sind von Gesetzes wegen oder aufgrund von geschäftlichen oder strategischer Anforderungen vor unrechtmässiger oder missbräuchlicher Datenbearbeitung zu schützen. Bei der unrechtmässigen Bearbeitung von vertraulichen Personendaten besteht die Gefahr von erheblichen negativen Folgen für die betroffene Person. Die allermeisten Personendaten fallen in diese Kategorie, sofern sie nicht bereits streng vertraulich klassifiziert sind. Das Risiko einer Persönlichkeitsverletzung ist anhand der Art und dem Kontext der Informationen zu analysieren. Es gelten hier strenge Vorschriften zum technischen und organisatorischen Schutz der Informationen und somit auch zur Vergabe von Zugriffsrechten.

*Beispiele **vertraulicher Informationen mit** Personendaten:*

- Baugesuchsverfahren mit nicht öffentlichen Personendaten wie Einsprachen zum Baugesuch
- Vertrauliche RRBs zu Mitarbeitenden mit Angaben zu persönlichen Zulagen.
- Preisverhandlungen der Liegenschaftsverwaltung mit möglichen Käufern der Kantonsliegenschaften und -Grundstücke.

*Beispiele **vertraulicher Informationen ohne** Personendaten:*

- Geplante Änderung der Linienführung im öffentlichen Verkehr vor der Publikation.
- Prüfungsfragen im Schul-/Universitätsbereich.

Weitere Beispiele zur Unterscheidung zwischen vertraulichen und streng vertraulichen Personendaten

Information		Vertraulichkeitsstufe	Begründung
a)	…nimmt nur koscheres Essen zu sich	streng vertraulich	Diese Angabe kann auf religiöse Ansichten schliessen lassen.
b)	… wohnt mit y an der Adresse (Name und Adresse)	Vertraulich, je nach Bezug streng vertraulich	In der Regel sind diese Angaben nicht streng vertraulich, sondern vertraulich. Um streng vertrauliche Informationen handelt es sich jedoch bspw., wenn: - sich Person x bspw. in einem Zeugenschutzprogramm befindet oder in einem Frauenhaus wohnt. - aus den Informationen zur Wohnadresse Rückschlüsse möglich sind, dass sich die Personen vermutlich in einer eingetragenen Partnerschaft befinden (besondere Personendaten betr. Intimsphäre).
c)	…bezieht Sozialhilfe	streng vertraulich	Diese Angabe zählt zu den besonderen Personendaten (Massnahmen der sozialen Hilfe).
d)	...hat ein steuerbares Einkommen von CHF 150‘000	streng vertraulich	Das Einkommen zählt zwar nicht zu den besonderen Personendaten untersteht aber dem kantonalen Steuergeheimnis (§ 111 ff Steuergesetz, SGS 331).

Information		Vertraulich-keitsstufe	Begründung
e)	…ist Mitglied in einer Gewerkschaft	streng vertraulich	Diese Angabe lässt auf gewerkschaftliche Ansichten oder Tätigkeiten schliessen und zählt somit zu den besonderen Personendaten.
f)	…ist wegen Trunkenheit am Steuer vorbestraft	streng vertraulich	Diese Angabe beinhaltet eine strafrechtliche Sanktion und zählt somit zu den besonderen Personendaten .
g)	… ist verheiratet	vertraulich	Diese Information ist anders als bei eingetragener Partnerschaft,welche implizit Angaben zur Intimsphäre enthält, nicht streng vertraulich.
h)	… wurde HIV-Positiv getestet	streng vertraulich	Dies ist eine medizinische Angabe zur Gesundheit (besonderes Personendatum) mit stigmatisierendem medizinischem Befund .
i)	…trägt eine Brille mit Dioptrie 1,5	streng vertraulich	Dies ist eine medizinische Angabe zur Gesundheit und damit grundsätzlich streng vertraulich. Die Risikobetrachtung betr. Verletzung der Privatsphäre kann in diesem Fall dazu führen, dass bei diesem Gesundheitsdatum keine erhöhten Schutzmassnahmen getroffen werden müssen.
j)	... wurde betrieben	vertraulich	Diese Angabe ist “nur“ vertraulich, da sie weder zu den besondere Personendaten zählt noch dazu eine spezielle gesetzliche Geheimhaltungspflicht besteht
k)	…wurde von der Schule ausgeschlossen	streng vertraulich	Es handelt sich dabei um eine administrative Sanktion und zählt somit zu den besonderen Personendaten (§ 3 Abs. 4 IDG).

Interne Informationen

Als „intern“ werden Informationen klassifiziert, die weder als „streng vertraulich“ noch als „vertraulich“ klassifiziert werden müssen, deren Inhalt jedoch aufgrund schutzwürdiger Interessen nicht für die Veröffentlichung bestimmt oder geeignet ist.. Interne Informationen mit Personenbezug enthalten in der Regel keine Personendaten von Dritten wie bspw. Einwohner. Eine mögliche Fehlinterpretation des Begriffs «intern» wäre die Klassifizierung von Personendaten, die nur intern in einer Behörde bearbeitet werden.

*Beispiele **interner Informationen mit** Personendaten:*

- Im Intranet wird eine Liste mit neueintretenden Mitarbeitenden veröffentlicht.
- Im Servicekatalog sind die Serviceverantwortlichen ersichtlich.

*Beispiele **interner Informationen ohne Personendaten**:*

- interne Weisungen und Richtlinien von bspw. Direktionen.
- Informatikvorhaben von Direktionen.

Nicht klassifizierte Informationen

Als „nicht klassifiziert" gelten Informationen, die keine spezielle Schutzbedarfsklasse haben, also weder intern, noch vertraulich, noch streng vertraulich klassifiziert sind. Es handelt sich demnach um öffentliche Informationen.

- Anonymisierte Polizeimeldungen.
- Öffentliche Landratsprotokolle.
- Medienmitteilungen zu RRBs.
- öffentliche Versteigerung von Autos, Motorrädern und Velos.

4.2. Verfügbarkeit[3]

Das Schutzziel „Verfügbarkeit" beschreibt, in welchem Umfang die Daten und Systeme bei Störungen und Ausfällen in dem vereinbarten Rahmen zu Verfügung stehen müssen.

Extrem hoch (Wiederanlaufzeit 0.5h)

- Das Einsatzleitsystem der Polizei benötigt eine extrem hohe Verfügbarkeit, weil die Polizei jederzeit einsatzbereit sein muss.
- Stehen Klinikinformationssysteme nicht zur Verfügung besteht potentiell eine Gefahr für Leib und Leben.

Sehr hoch (Wiederanlaufzeit 4h)

- Der Fach-Service Polycom als nationales Funksystem der Behörden und Organisationen für Rettung und Sicherheit ist strategisch und weist eine sehr hohe Verfügbarkeit auf.
- Das Meldungsvermittlungssystem VULPUS ist bei der Polizei in ordentlichen, besonderen und ausserordentlichen Lage stets im Dauerbetrieb und ist folglich sehr hoch verfügbar.

Hoch (Wiederanlaufzeit 24h)

- Der Fach-Service Geo-Dienste stellt Bürgern, den Gemeinden und den Mitarbeitenden der kantonalen Verwaltung den Zugriff auf die verschiedensten Geo-Dienste auch ausserhalb der regulären Arbeitszeiten zur Verfügung und weist deshalb eine hohe Verfügbarkeit auf.
- E-Mail hat sich als wichtiges Kommunikationsmittel etabliert, auch ausserhalb der Arbeitszeiten. Der Basis-Service E-Mail ist deshalb hoch verfügbar.

Normal (Wiederanlaufzeit 72h)

- Der Fach-Service Wehrpflichtersatz wird während der Bürozeiten benötigt und weist eine normale Verfügbarkeit aus.

[3] Die Beispiele zur Verfügbarkeit wurden uns vom kantonalen SIBE bei der Zentralen Informatik zur Verfügung gestellt.

4.3. Integrität

Das Schutzziel Integrität beschreibt die Anforderungen an die Richtigkeit (Korrektheit / Unversehrtheit) von Informationen und damit zusammenhängend der korrekten Funktionsweise von Systemen.

Erhöhte Anforderungen an die Integrität

Bei „erhöhten Anforderungen" muss ein Fehler sofort erkannt werden, da die Informationen unmittelbar Handlungen auslösen, die nicht mehr rückgängig gemacht werden können, die aber bei falschen Angaben fatale Folgen haben können.

- Medizinische Daten müssen zwingend richtig sein (z.Bsp. Informationen zu Allergien, Medikationen etc.).
- Die Anforderungen an die Richtigkeit der Daten bei Strafverfolgungen sind erhöht.
- Die Personendaten im kantonalen Personenregister arbo müssen richtig sein, da sich daraus Ansprüche (z.B. Ergänzungsleistungen, IV) ableiten.
- Elektronische Übermittlung von Dokumenten im Rahmen von Zivil- und Strafprozessen sowie Schuldbetreibungs- und Konkursverfahren

Normale Anforderungen an die Integrität

Bei „normalen Anforderungen" ist die Richtigkeit der Daten von der Sache her sehr wichtig. Tritt aber dennoch ein Fehler auf, kann mit entsprechendem Aufwand die Integrität wieder hergestellt werden. Die Integritätsverletzung ist letztlich korrigierbar. Fehler in den Daten sind zwar nicht erwünscht, können aber erkannt und bereinigt werden. Der Geschäftsprozess kann bis dahin auch bei fehlerhaften Informationen korrekt durchgeführt werden.

- Fehler in einer Lohnabrechnung (z.B. fehlende oder falsche Spesengutschriften können mit der Folgeabrechnung korrigiert werden.).
- Fristerstreckungsgesuch einer Privatperson zur Abgabe der Steuererklärung.

4.4. Nachvollziehbarkeit

Das Schutzziel Nachvollziehbarkeit dient der Rückverfolgung der Datenbearbeitung (Lesen, Schreiben, Löschen, etc.) und der Zurechenbarkeit dieser zu einer bestimmten Person. Die Anforderungen dazu leiten sich einerseits aus §§ 9 und 11 IDG sowie § 4 Abs. 1 Archivierungsgesetz ab. Auch in Fachgesetzen gibt es Normen dazu (z.B. ARG/ARV, SGS 111 resp. 111.11).

Erhöhte Anforderungen an die Nachvollziehbarkeit

Bei „erhöhten Anforderungen" besteht eine gesetzliche Vorgabe oder geschäftliche Anforderung jeden Zugriff einer eindeutig authentifizierten Identität und/oder jeden Zugriff lückenlos zuordnen zu können.

- Dort, wo im Rahmen von Abrufverfahren die jeweilige Berechtigung der konkreten Abfrage nicht ad hoc überprüft werden kann, muss deren Rechtmässigkeit in Stichprobenkontrollen nachvollzogen werden können. So muss jede Abfrage aus dem kantonalen Personenregister arbo elektronisch protokolliert werden, um die Rechtmässigkeit der Datenbearbeitung nachvollziehen zu können (§ 27 ARV). Ähnlich bei Zugriffen auf das elektronische Personaldossier (§ 3 Verordnung über den Umgang mit Personaldaten, SGS 150.21)).
- Im System „Betreibungsregister Online" besteht eine erhöhte Anforderung an die Nachvollziehbarkeit: Es muss nachvollziehbar sein, wer welche Betreibung eingereicht hat.
- Bei der elektronischen Übermittlung von Dokumenten im Rahmen von Zivil- und Strafprozessen sowie Schuldbetreibungs- und Konkursverfahren besteht eine gesetzliche Vorgabe, jeden Bearbeitungsschritt einer eindeutig authentifizierten Identität so zuordnen und jeden Bearbeitungsschritt lückenlos so nachvollziehen zu können, dass die Qualität eines richterlichen anerkannten Belegs erreicht wird.

Normale Anforderungen an die Nachvollziehbarkeit

Unter „normalen Anforderungen" versteht man Aktivitäten, bei denen ein normaler Bedarf nach Nachvollziehbarkeit besteht. Um Änderungen an IT-Systemen nachvollziehen zu können, werden diese Änderungen an Systemkonfigurationen protokolliert

- Hinzugefügte oder geänderte Inhalte im Intranet- / Internet-Auftritt BL.

Version 1.9 ASD / 15.8.2024

Aufsichtsstelle Datenschutz

Kanonengasse 20
4410 Liestal

T 061 552 64 30

datenschutz@bl.ch

www.bl.ch/datenschutz