

Datenschutzkonzept der Biffig AG

1.	Zweck und Umfang.....	2
2.	Gesetzliche Grundlagen	2
3.	Begriffe	2
4.	Geltungsbereich.....	2
5.	Zielsetzung	3
6.	Grundsätze des Datenschutzes	3
6.1	Rechtmässigkeit	3
6.2	Verhältnismässigkeit.....	3
6.3	Zweckbindung.....	3
6.4	Transparenz.....	3
6.5	Datenqualität.....	3
6.6	Treu und Glauben.....	3
7.	Massnahmen zur Datensicherheit.....	3
7.1	Organisatorische Massnahmen.....	4
7.2	Technische Massnahmen.....	4
7.3	Archivierung.....	4
7.4	Vernichtung.....	4
8.	Datenschutz-Folgenabschätzung	4
9.	Bearbeitung im Auftrag	5
9.1	Allgemeines	5
9.2	Bestimmungen für Auftraggeber (die Biffig AG)	5
9.3	Bestimmungen für Auftragnehmer.....	5
10.	Verletzung der Datensicherheit	5
10.1	Interne Meldepflicht	5
10.2	Nachforschung und Sicherheitsmassnahmen.....	6
10.3	Meldung an die Datenschutz-Aufsichtsbehörde.....	6
10.4	Benachrichtigung von betroffenen Personen	6
11.	Rechte der betroffenen Personen	6
11.1	Aufklärung/Orientierung.....	6
11.2	Auskunfts-/Einsichtsrecht	6
11.3	Recht auf Berichtigung	7
11.4	Recht auf Vernichtung	7
11.5	Sperrung/Verweigerung der Datenbekanntgabe.....	7
12.	Handlungsanleitungen	7
12.1	Verhalten bei telefonischen und schriftlichen Anfragen	7
12.2	Grundsätze der E-Mail-Nutzung	7
12.3	Verwendung von Bild-/Tonaufnahmen	8
13.	Verantwortlichkeiten	8
13.1	Verwaltungsrat.....	8
13.2	Geschäftsleitung	8
13.3	Datenschutzkoordinator :in (DSK)	8
13.4	Leitung HR.....	9
13.5	Führungspersonen	9
13.6	Mitarbeitende	9
14.	Anhang 1: Begriffe.....	10

1. Zweck und Umfang

Das vorliegende Datenschutzkonzept der Biffig AG trägt der Bedeutung und dem Stellenwert des Datenschutzes im Sinne der Achtung der Privatsphäre und der Persönlichkeitsrechte ihrer Bewohnenden, ihrer Mitarbeitenden und allenfalls auch ihrer Geschäftspartner:innen Rechnung. Es bildet die verbindliche Grundlage für alle datenschutzrelevanten Massnahmen und Aktivitäten in der Biffig AG, namentlich für das Bearbeiten von

- Personendaten der Bewohnenden;
- Personendaten der Mitarbeitenden, inklusive Daten über Stellenbewerber:innen und ehemalige Mitarbeitende;
- Informationen über Geschäftspartner:innen und weitere Dritte, soweit Personendaten betroffen sind.

2. Gesetzliche Grundlagen

Dieses Datenschutzkonzept richtet sich nach den Bestimmungen der Datenschutzgesetze des Bundes und des Kantons Luzern.

Dies sind:

- Bundesgesetz über den Datenschutz (DSG; SR 235.1)
- Verordnung über den Datenschutz (DSV; SR 235.11)
- Kantonales Gesetz über den Schutz von Personendaten (Kantonales Datenschutzgesetz, KDSG; SRL Nr. 38)
- Kantonale Datenschutzverordnung (KDSV; SRL Nr. 38b)

Weiter sind datenschutzrechtliche Bestimmungen in den verschiedenen Spezialgesetzen und -verordnungen (insbesondere im Gesundheitsrecht) zu beachten.

Im Bereich des privatwirtschaftlichen Handelns untersteht die Biffig AG grundsätzlich der Datenschutzgesetzgebung des Bundes.

Soweit die Biffig AG Leistungen im Zusammenhang mit der Grundversicherung erbringt bzw. einen kantonalen Leistungsauftrag erfüllt, sind die Bestimmungen des kantonalen Datenschutzgesetzes anwendbar.

3. Begriffe

Wichtige Begriffe sind im Anhang 1 definiert.

4. Geltungsbereich

Das vorliegende Datenschutzkonzept gilt für alle Organe und Mitarbeiter:innen der Biffig AG, die im Rahmen der Erfüllung ihrer Funktionen und Aufgaben Personendaten bearbeiten.

Es gilt ebenfalls für externe Personen und Firmen, sofern sie sich durch entsprechende schriftliche Vereinbarung zu dessen Einhaltung verpflichten.

5. Zielsetzung

Das Hauptziel dieses Konzepts ist die Gewährleistung des Schutzes der Persönlichkeit natürlicher Personen vor widerrechtlicher oder unverhältnismässiger Bearbeitung der Daten von Personen gemäss Ziffer 1. Dieses Konzept soll als verbindliche Richtlinie für alle bei der Biffig AG tätigen Personen gelten und als Unterstützung dienen in Eigenverantwortung datenschutzrechtlich die Biffig AG vor materiellen Nachteilen und Imageschäden zu schützen, welche ihr aufgrund von datenschutzwidrigen Handlungen entstehen könnten.

6. Grundsätze des Datenschutzes

6.1 Rechtmässigkeit

Rechtmässig ist die Datenbearbeitung, wenn sie durch die Einwilligung der betroffenen Person, eine gesetzliche Ermächtigung oder ein überwiegendes öffentliches oder privates Interesse gerechtfertigt ist.

6.2 Verhältnismässigkeit

Die Datenerhebung muss erforderlich sein, zudem soll ein überwiegendes Interesse an der Erhebung bestehen. Datenerhebungen auf Vorrat sind widerrechtlich, nicht mehr benötigte Daten sind zu vernichten.

6.3 Zweckbindung

Die Daten dürfen nur zum Zweck bearbeitet werden, der bei der Erhebung der Daten genannt wurde. Ihre Daten dürfen zu keinem für die betroffene Person nicht erkennbaren Zweck bearbeitet werden.

6.4 Transparenz

Die Datenerhebung und -bearbeitung muss klar erkennbar sein. Die notwendigen Informationen sollen direkt bei der betroffenen Person beschafft werden.

6.5 Datenqualität

Es muss sichergestellt sein, dass die bearbeiteten Daten richtig, vollständig und aktuell sind. Unrichtige und unvollständige Daten sind zu korrigieren oder zu vernichten.

6.6 Treu und Glauben

Widersprüchliches und rechtmisbräuchliches Verhalten ist unzulässig.

7. Massnahmen zur Datensicherheit

Mit organisatorischen und technischen Massnahmen sollen der Datenschutz gewährleistet und Personendaten insbesondere vor dem Zugang Unbefugter, Missbrauch, Vernichtung, Verlust, technischen Fehlern, Fälschung, Diebstahl etc. geschützt werden.

7.1 Organisatorische Massnahmen

Zugang zu Personendaten besteht bei der Biffig AG nach dem Grundsatz «So viel wie nötig, so wenig wie möglich».

Die/Der Datenschutzkoordinator:in (DSK) schlägt deshalb in Zusammenarbeit mit den jeweils zuständigen Führungspersonen für jede Datensammlung vor, wer unter welchen Bedingungen Zugang zu Personendaten hat und wie dies überwacht wird.

Sie/Er führt ein Verzeichnis der Bearbeitungstätigkeiten gemäss den gesetzlichen Anforderungen und hält dieses aktuell.

Sie/Er überprüft zudem, wem Zugang zu archivierten Daten gewährt wird.

7.2 Technische Massnahmen

Der Schutz elektronisch bearbeiteter Daten wird insbesondere durch die Verwendung und regelmässige umfassende Verschlüsselung, den Einsatz von Firewalls, Virenschutzprogrammen etc. und die Protokollierung von Zugriffen gewährleistet.

Durch Zugangs- und Personendatenträgerkontrollen wird verhindert, dass unbefugte Personen Zugang zu Datenbeständen haben oder diese verändern, zerstören, entwenden etc.

7.3 Archivierung

Personendaten, die für die Bearbeitung nicht mehr benötigt werden, werden gemäss den Richtlinien der/des Datenschutzverantwortlichen aufbereitet und während der definierten Dauer archiviert.

7.4 Vernichtung

Daten von untergeordneter Bedeutung werden unmittelbar nach Erreichen des Bearbeitungszwecks vernichtet (physisch zerstört oder elektronisch gelöscht)

8. Datenschutz-Folgenabschätzung

Die Biffig AG analysiert bei der Einführung neuer Bearbeitungsvorgänge oder bei einer wesentlichen Änderung eines bestehenden Bearbeitungsvorganges vor der Bearbeitung, insbesondere durch die Verwendung neuer Technologien, ob diese Bearbeitung ein hohes Risiko für die Grundrechte der Betroffenen darstellt. Dabei sind Art, Umfang, Kontext und Zweck der Datenbearbeitung zu berücksichtigen.

Im Rahmen der Risikoanalyse führt die Biffig AG eine Bewertung der Auswirkungen der geplanten Bearbeitungen auf den Schutz von Personendaten durch (Datenschutz-Folgenabschätzung).

Besteht nach Durchführung der Datenschutz-Folgenabschätzung und der Anwendung geeigneter Massnahmen zur Risikominderung ein hohes Risiko für die Rechte und Freiheiten der Betroffenen, muss der / die DSK die zuständige Datenschutzaufsichtsbehörde konsultieren (Vorab-Konsultation).

9. Bearbeitung im Auftrag

9.1 Allgemeines

Eine Auftragsbearbeitung liegt vor, wenn ein Auftragnehmer Personendaten im Namen und nach Weisung der Biffig AG (Auftraggeber) bearbeitet. In diesen Fällen ist eine Vereinbarung über eine Auftragsbearbeitung abzuschliessen gemäss den einschlägigen gesetzlichen Anforderungen.

Dabei behält die Biffig AG die volle Verantwortung für die korrekte Durchführung der Datenbearbeitung.

9.2 Bestimmungen für Auftraggeber (die Biffig AG)

Bei der Erteilung des Auftrags sind die nachfolgenden Vorgaben einzuhalten:

- Der Auftragnehmer ist nach seiner Eignung zur Gewährleistung der erforderlichen technischen und organisatorischen Schutzmassnahmen auszuwählen;
- Der Auftrag ist schriftlich zu erteilen;
- Die Biffig AG muss sich vor Beginn der Datenbearbeitung durch geeignete Prüfung vergewissern, dass der Auftragnehmer die vorgenannten Pflichten erfüllt. Ein Auftragnehmer kann seine Einhaltung der Datenschutzanforderungen insbesondere durch eine entsprechende Zertifizierung dokumentieren. Je nach Risiko der Datenbearbeitung müssen Prüfungen während der Vertragslaufzeit regelmässig wiederholt werden;
- Eine grenzüberschreitende Auftragsdatenbearbeitung ist nur zulässig, wenn der Auftragnehmer ein zu diesem Datenschutzkonzept gleichwertiges Datenschutzniveau nachweist.

9.3 Bestimmungen für Auftragnehmer

Der Auftragnehmer darf Personendaten nur im Rahmen der Weisungen von der Biffig AG als Auftraggeber bearbeiten.

Der Auftragnehmer darf Dritte («Unterauftragnehmer») zur Bearbeitung von Personendaten im eigenen (Unter-)Auftrag nur mit vorherigem Einverständnis vom der Biffig AG beauftragen. Das Einverständnis darf nur erteilt werden, wenn der Auftragnehmer dem Unterauftragnehmer vertraglich die gleichen Datenschutzpflichten, die dem Auftragnehmer nach Massgabe dieses Konzepts gegenüber der Biffig AG und den Betroffenen obliegen, und angemessene technische und organisatorische Schutzmassnahmen auferlegt. Die Form des Einverständnisses sowie Informationspflichten bei Änderungen im Unterauftragsverhältnis sind im Dienstleistungsvertrag zu regeln.

10. Verletzung der Datensicherheit

Eine Verletzung der Datensicherheit (Datenschutzvorfall) liegt vor, wenn Personendaten unwiederbringlich vernichtet werden bzw. verloren gehen, oder unbeabsichtigt oder unrechtmässig verändert bzw. offenbart werden oder Unbefugten zugänglich werden.

10.1 Interne Meldepflicht

Wurde eine Datenschutzverletzung festgestellt oder vermutet, ist jeder Mitarbeitender verpflichtet, dies unverzüglich dem / der DSK mitzuteilen, insbesondere bei schwerwiegenden Datenschutzverletzungen und solchen, bei denen zum Schutz der Betroffenen Schutzmassnahmen durch die Biffig AG getroffen werden müssen.

Die Meldung kann in jeder Form erfolgen; bei mündlichen Meldungen sind diese unverzüglich schriftlich

nachzuholen.

10.2 Nachforschung und Sicherheitsmassnahmen

Handelt es sich bei der Meldung um einen Verdacht einer Verletzung der Datensicherheit, leitet der / die DSK unverzüglich etwaig erforderliche Nachforschungsmassnahmen ein und informiert unverzüglich die Geschäftsleitung. Gleiches gilt, wenn die wahrscheinlichen Folgen der Datenschutzverletzung und damit das mögliche Risiko der Datenschutzverletzung unklar sind.

Soweit erforderlich leitet der / die DSK bzw. die Geschäftsleitung sofort Massnahmen (z.B. Sperrung von Zugängen, Änderung von Passwörtern, Einspielen von Backups) zur Behebung der Datenschutzverletzung oder zur Abmilderung möglicher nachteiliger Auswirkungen der Verletzung der Datensicherheit.

10.3 Meldung an die Datenschutz-Aufsichtsbehörde

Der / Die DSK muss entsprechende Ereignisse unverzüglich der zuständigen Aufsichtsbehörde melden, wenn die Verletzung der Datensicherheit zu einer Gefährdung der Grundrechte auf informationelle Selbstbestimmung bzw. auf Privatsphäre von betroffenen Personen führen kann. Bestehen Zweifel, ob Grundrechte der Betroffenen gefährdet sind, ist ebenfalls Meldung zu erstatten.

10.4 Benachrichtigung von betroffenen Personen

Zusätzlich müssen die betroffenen Personen benachrichtigt werden, wenn es zu deren Schutz erforderlich ist. Für die Benachrichtigung ist der / die DSK verantwortlich, der sich hierzu mit der Geschäftsleitung abstimmt.

11. Rechte der betroffenen Personen

Dem Ziel, im Alltag regelmässig eintretende Situationen datenschutzrechtlich korrekt zu handhaben, dienen die folgenden Handlungsanleitungen.

11.1 Aufklärung/Orientierung

Bewohnende sowie Mitarbeitende werden beim Eintritt über ihre datenschutzrechtlichen Rechte und Pflichten informiert.

Der/Die DSK orientiert sie angemessen über die Beschaffung sie betreffender Personendaten.

11.2 Auskunfts-/Einsichtsrecht

Die von der Bearbeitung ihrer Daten betroffene Person darf über Erhebung, Herkunft, Inhalt, Zweck, Kategorie und Rechtsgrundlage Auskunft verlangen und in die Datensammlung Einsicht zu nehmen. Sie hat auch das Recht auf die Bekanntgabe der an der Sammlung Beteiligten und Datenempfänger.

Die Auskunft bzw. Einsicht verlangende Person muss sich über ihre Identität ausweisen.

Die Auskunft ist innert 30 Tagen in allgemeinverständlicher Weise, schriftlich und kostenlos zu erteilen.

Die Erteilung von Auskünften und die Einsichtsrechte dürfen ausnahmsweise beschränkt oder verweigert werden, wenn wichtige und überwiegende öffentliche Interessen oder besonders schützenswerte Interessen von Dritten entgegenstehen.

Besteht das Risiko, dass die betroffene Person (v.a. Minderjährige) mit der Auskunftserteilung oder Einsichtnahme einer zu hohen Belastung ausgesetzt werden könnte, kann sie eine andere Person

bestimmen, der an ihrer Stelle Auskunft erteilt bzw. Einsicht gewährt wird.

Die Auskunftserteilung und das Einsichtsrecht werden über eine zentrale Stelle abgewickelt.

11.3 Recht auf Berichtigung

Widerrechtlich oder unrichtig bearbeitete sowie unrichtige Daten müssen berichtigt oder vernichtet werden.

11.4 Recht auf Vernichtung

Jede betroffene Person ist berechtigt, die Vernichtung bzw. Löschung ihrer Personendaten zu verlangen.

Wenn Personendaten unrechtmässig erhoben wurden oder die Personendaten für den Zweck, für den sie erhoben oder sonst bearbeitet werden, nicht mehr benötigt werden, sind diese zu vernichten bzw. zu löschen. Bestehende gesetzliche Aufbewahrungspflichten und einer Vernichtung- bzw. Löschung entgegenstehende schutzwürdige Interessen müssen beachtet werden.

11.5 Sperrung/Verweigerung der Datenbekanntgabe

Jede betroffene Person kann die Bekanntgabe ihrer Daten sperren lassen, wenn sie ein schutzwürdiges Interesse nachweist. Dies gilt dann nicht, wenn die Datenbekanntgabe eine gesetzliche Verpflichtung darstellt, aufgrund überwiegender Interessen Dritter erforderlich ist oder zur Aufklärung von mutmasslich rechtsmissbräuchlichen Handlungen der betroffenen Person erforderlich ist.

12. Handlungsanleitungen

Dem Ziel, dass im Alltag regelmässig eintretende Situationen datenschutzrechtlich korrekt gehandhabt werden, dienen die folgenden Handlungsanleitungen:

12.1 Verhalten bei telefonischen und schriftlichen Anfragen

Ohne ausdrückliche Einwilligung der betroffenen Person oder ohne entsprechende gesetzliche Erlaubnis dürfen Personendaten nicht an Aussenstehende weitergegeben werden.

Bei telefonischen Anfragen ist die eindeutige Identifizierung der anfragenden Person sicherzustellen. Werden Telefongespräche aufgezeichnet, muss darauf hingewiesen werden und die Zustimmung des/der Gesprächspartner:in eingeholt werden.

12.2 Grundsätze der E-Mail-Nutzung

E-Mails können durch Dritte mitgelesen oder verändert werden. Grundsätzlich sollen deshalb möglichst wenig Personendaten per E-Mail übermittelt werden und sie sollen keine sensiblen Informationen oder Angaben über Passwörter und andere Zugangsdaten enthalten.

Per E-Mail dürfen besonders schützenswerte Daten grundsätzlich nur verschlüsselt übermittelt werden, sofern die betroffene Person keine gegenteilige, schriftliche Erklärung abgegeben hat.

Zu beruflichen Zwecken bearbeitete Personendaten dürfen nicht auf privaten Geräten gespeichert werden.

12.3 Verwendung von Bild-/Tonaufnahmen

Auf Bild-, Film- und/oder Tonaufnahmen erkennbar dürfen nur Personen festgehalten werden, welche dazu ihre Einwilligung gegeben haben.

Die Einwilligung der betroffenen Person muss freiwillig, ausdrücklich und nach vorgängiger Aufklärung über den Zweck und die Verwendung der Aufnahmen erfolgen. Die Zustimmung kann schriftlich oder – bei Anwesenheit mehrerer Personen – mündlich oder nonverbal erfolgen und ist zu dokumentieren.

13. Verantwortlichkeiten

13.1 Verwaltungsrat

Der Verwaltungsrat ist auf strategischer Ebene für die Gewährleistung des Datenschutzes bei der Biffig AG verantwortlich.

Er nimmt den Datenschutz als relevantes Thema in ihr Risikomanagement-System auf und beurteilt die entsprechenden Risiken in strategisch stufengerechter Weise.

Er erlässt das vorliegende Datenschutzkonzept und überprüft dieses regelmässig.

Er bestimmt die/den Datenschutzkoordinator:in, regelt ihre/seine Aufgaben, Verantwortlichkeiten und Kompetenzen unter Berücksichtigung der Vorschriften der Gesetzgebung in einem Pflichtenheft und nimmt ihre/seine regelmässige Berichterstattung entgegen. Die Bestimmung kann an die Geschäftsleitung delegiert werden.

13.2 Geschäftsleitung

Die Geschäftsleitung ist in Zusammenarbeit mit der/dem DSK zuständig für die Umsetzung dieses Konzepts und für die Einhaltung der datenschutzrechtlichen Vorgaben im Rahmen aller Datenbearbeitungen auf operativer Ebene.

Sie sorgt in geeigneter Weise dafür, dass alle Mitarbeitenden regelmässig für die Belange des Datenschutzes sensibilisiert und über die Vorgaben dieses Konzepts und deren Anwendung im beruflichen Alltag informiert werden.

Sie sorgt für eine regelmässige Information an die strategische Leitung.

13.3 Datenschutzkoordinator :in (DSK)

Die/Der DSK nimmt betriebsintern die Aufgaben gemäss der Gesetzgebung und dem Pflichtenheft wahr.

Sie/Er ist nach innen und aussen die Ansprechperson für alle Fragen bezüglich des Datenschutzes.

Sie/Er prüft die Rechtmässigkeit der Datenbearbeitung bei der Biffig AG.

Sie/Er kann Massnahmen empfehlen, soweit dies für die Einhaltung der Gesetzgebung und die Umsetzung dieses Konzepts erforderlich ist.

Sie/Er erstattet gegebenenfalls Meldungen an die Datenschutzbeauftragten des Bundes und/oder des Kantons.

Sie/Er berichtet der Geschäftsleitung regelmässig über die Datenbearbeitung in der Biffig AG, weist dabei auf erkannte Risiken hin und gibt Empfehlungen für mögliche Verbesserungen ab. Über besondere Vorkommnisse von grösserer Tragweite orientiert sie/er unverzüglich.

Sie/Er führt regelmässige Datenschutz-Audits durch und zieht hierfür auf Antrag bei Bedarf externe Unterstützung bei.

Sie/Er steht dem Verwaltungsrat, der Geschäftsleitung, der Leitung HR, den Mitarbeitenden sowie den Bewohnenden bei datenschutzrechtlichen Fragen beratend zur Verfügung.

13.4 Leitung HR

Die Leitung HR ist für die sorgfältige und datenschutzkonforme Bearbeitung der Personendaten der Mitarbeitenden im Rahmen der Personalarbeit verantwortlich.

13.5 Führungspersonen

Die Vorgesetzten aller Stufen nehmen eine Vorbildfunktion wahr und fördern die Motivation der Mitarbeitenden, dem Datenschutz bei ihrem Handeln am Arbeitsplatz Rechnung zu tragen.

Sie sind in ihren Verantwortungsbereichen für die Durchsetzung und Einhaltung des Datenschutzes verantwortlich, insbesondere im Rahmen dieses Konzepts und der Geschäftsprozesse.

Sie sorgen in Zusammenarbeit mit der/dem DSK für die datenschutzgemässige Sensibilisierung und handlungsorientierte Anleitung der Mitarbeitenden.

13.6 Mitarbeitende

Alle Mitarbeitenden der Biffig AG, welche Personendaten bearbeiten, tragen dem Datenschutz eigenverantwortlich Rechnung und handeln dabei insbesondere gemäss dem vorliegenden Konzept und den Weisungen der/des DSK.

Sie wenden sich bei Fragen und Unsicherheiten an ihre Vorgesetzten oder an die/den DSK.

Dieses Konzept gilt ab sofort.

Schötz, 09.11.2023

Biffig AG



Stefan Wülser
Geschäftsführer



Priska Eigensatz
Bereichsleitung Kundenservice & Dienste

14. Anhang 1: Begriffe

Personendaten	Angaben über eine bestimmte oder bestimmbare natürliche Person.
Besonders schützenswerte Personendaten	<ul style="list-style-type: none"> a) Daten über religiöse, weltanschauliche, politische oder gewerkschaftliche Ansichten oder Tätigkeiten; b) Daten über die Gesundheit, die Intimsphäre oder die Zugehörigkeit zu einer ethnischen Gruppe oder Herkunft; c) genetische Daten; d) biometrische Daten, die eine natürliche Person eindeutig identifizieren; e) Daten über verwaltungs- und strafrechtliche Verfolgung oder Sanktionen; f) Daten über Massnahmen der sozialen Hilfe.
Bearbeiten von Personendaten	Jeder Umgang mit Personendaten, unabhängig von den angewandten Mitteln und Verfahren, wie das Beschaffen, Speichern, Verwenden, Verändern, Bekanntgeben, Archivieren, Löschen oder Vernichten von Daten.
Bekanntgabe von Personendaten	Jedes Übermitteln oder Zugänglichmachen von Personendaten.
Datensammlung	Bestand von Personendaten, der so aufgebaut ist, dass die Daten nach bestimmten Personen erschliessbar sind.
Datenschutzkoordinator:in	Person, welche betriebsintern die Einhaltung der Datenschutzvorschriften überwacht und u.a. ein Verzeichnis der Datensammlungen führt.
Inhaber/in der Datensammlung	Verantwortliche/r für eine Datenbearbeitung. Sie/Er entscheidet allein oder zusammen mit anderen über den Zweck und die Mittel der Bearbeitung.
Persönlichkeitsprofil	Zusammenstellung von Daten, die eine Beurteilung wesentlicher Aspekte der Persönlichkeit einer natürlichen Person erlaubt.
Profiling	Bewertung bestimmter Merkmale einer Person aufgrund von automatisiert bearbeiteten Personendaten (um z.B. die Arbeitsleistung, die wirtschaftlichen Verhältnisse, die Gesundheit, das Verhalten, bestimmte Vorlieben, den Aufenthaltsort oder die Mobilität zu analysieren oder vorherzusagen).