



Von Internet, Personal- dossiers & Co.

12 Fälle zum Datenschutz im Personalbereich

Inhalt

Vorwort	4
Personaldossier	5
1 Welche Unterlagen gehören in ein Personaldossier?	5
2 Wer hat Einsicht ins Personaldossier?	5
3 Dürfen Mitarbeitende in alle Unterlagen ihres Personaldossiers Einsicht nehmen?	6
4 Was können Mitarbeitende gegen die Bearbeitung unrichtiger Daten tun?	6
Internet / E-Mail / Überwachung	5
5 Dürfen Fotos von Mitarbeitenden im Internet veröffentlicht werden?	7
6 Welche Vorkehrungen im Umgang mit E-Mail sind für den Fall der Abwesenheit von Mitarbeitenden zu beachten?	8
7 Darf die Arbeitgeberin oder der Arbeitgeber Internetgebrauch und E-Mail-Verkehr kontrollieren?	9
8 Was müssen Vorgesetzte bei einem Verdacht auf eine Straftat beachten?	9
Mitarbeiterumfrage	10
9 Unter welchen Voraussetzungen darf eine Mitarbeiterumfrage durchgeführt werden?	10
10 Besteht die Pflicht zur Teilnahme an einer Mitarbeiterumfrage?	11

Verschiedenes	11
11 Ist es zulässig, eine Schulung mit nicht anonymisierten Personendaten durchzuführen?	11
12 Ist es zulässig, private Handy-Nummern auf einem internen Mitarbeitenden-Verzeichnis aufzuführen?	12
Glossar	13
Rechtsgrundlagen und Richtlinien	14
Grundsätze	15

Von Internet, Personaldossiers & Co. –

12 Fälle zum Datenschutz im Personalbereich

Leistungsbeurteilung, Gesundheitsdaten, Weiterbildung - im Personalbereich werden zahlreiche, auch besonders schützenswerte Personendaten bearbeitet. Ihre Verknüpfung ist aufgrund der rasanten technischen Entwicklung immer einfacher. Einerseits muss die Arbeitgeberin oder der Arbeitgeber Daten der Mitarbeitenden zur Durchführung des Arbeitsverhältnisses bearbeiten. Gleichzeitig ist die Arbeitgeberin oder der Arbeitgeber verpflichtet, eines der kostbarsten Güter der Mitarbeitenden, die Privatsphäre, zu schützen.

Datenvermeidung, Datensparsamkeit und die Einsetzung von datenschutzfreundlicher Technik sind wichtige Gebote, um die Persönlichkeit von Mitarbeitenden zu schützen. Die Arbeitgeberin oder der Arbeitgeber kann durch Transparenz bei

der Datenbearbeitung das Vertrauen der Mitarbeitenden erhöhen.

12 ausgewählte Fälle sollen den Datenschutz im Personalbereich veranschaulichen und dabei helfen, die schwierige Gratwanderung zwischen Interessen der Mitarbeitenden und Arbeitgebenden zu meistern.

Fachstelle Datenschutz
Personalamt

Juli 2020

Personaldossier¹

1 Welche Unterlagen gehören in ein Personaldossier?

Das Personaldossier beinhaltet ausschliesslich Unterlagen, die zur Durchführung des Arbeitsverhältnisses erforderlich sind. Ein Personaldossier kann zum Beispiel folgende Unterlagen beinhalten: Bewerbungsdossier, Referenzauskünfte, Stellenbeschreibung, Personalien, Adressdaten, Arbeitsvertrag, Standortgespräch, Unterlagen zur Weiterbildung, Arztzeugnis, Arbeitszeugnis und Korrespondenz.

Beim Personaldossier handelt es sich um ein Persönlichkeitsprofil, weshalb besondere Sorgfalt im Umgang damit gefordert ist, beispielsweise was die Aufbewahrung,

¹ Siehe auch Richtlinie zum Umgang mit Personalunterlagen und Personaldossiers unter Einbezug der datenschutzrechtlichen und der archivrechtlichen Bestimmungen, PHB SG 35.1.

die Zugriffsberechtigungen oder die technischen Massnahmen zur Sicherung der Daten anbelangt.

2 Wer hat Einsicht ins Personaldossier?

Einsicht in das Personaldossier dürfen Personen haben, welche die Daten für die Erfüllung des Arbeitsverhältnisses benötigen. Dazu zählen insbesondere Vorgesetzte und Personalverantwortliche. Die Daten müssen für die Aufgabenerfüllung geeignet und notwendig sein.² D.h., es besteht jeweils ein nur auf die konkrete Aufgabenerfüllung begrenztes Einsichtsrecht. Die betroffene Person selbst hat in alle ihre Daten Einsicht, wenn nicht öffentliche oder schutzwürdige private Interessen überwiegen oder ein Gesetz im formellen Sinn dies

² Art. 56 Abs. 1 Personalgesetz, sGS 143.1

vorsieht (siehe auch nachfolgendes Beispiel Ziff. 3).

3 Dürfen Mitarbeitende in alle Unterlagen ihres Personaldossiers Einsicht nehmen?

Grundsätzlich ja. Eine Ausnahme bilden Unterlagen, die ausschliesslich der persönlichen Gedankenstütze der vorgesetzten Person dienen (z.B. Notizen, wie ein Gespräch ablaufen soll). In Einzelfällen muss eine Abwägung zwischen den Interessen der betroffenen Person und schutzwürdigen privaten Interessen Dritter vorgenommen werden. Dies kann beispielsweise der Fall sein, wenn die Arbeitgeberin oder der Arbeitgeber ein Graphologie-Gutachten erstellen liess. Es wäre aber unverhältnismässig, die Einsicht in das ganze Gutachten zu verweigern. Vielmehr genügt, die

Einsicht zu beschränken, in dem der Name der Graphologin oder des Graphologen abgedeckt wird. Zudem kann die Auskunft oder Einsichtnahme eingeschränkt, verweigert oder mit Auflagen versehen werden, wenn ein Gesetz im formellen Sinn dies vorsieht.³

4 Was können Mitarbeitende gegen die Bearbeitung unrichtiger Daten tun?

Die Arbeitgeberin oder der Arbeitgeber darf über die Mitarbeitenden nur richtige Daten bearbeiten. Mitarbeiterinnen und Mitarbeiter können verlangen, dass das Organ, welche die Daten bearbeitet, unrichtige Personendaten kostenlos berichtigt. Kann weder Richtigkeit noch Unrichtigkeit bewiesen werden, bringt das öffentliche Organ

³ Art. 18 Datenschutzgesetz (DSG), sGS 142.1

bei den Personendaten einen entsprechenden Vermerk an und schränkt deren Bearbeitung ein.⁴ Dies ist zum Beispiel bei Werturteilen der Fall. Die betroffene Person kann dann einen Bestreitungsvermerk anbringen lassen.⁵

Internet / E-Mail / Ueberwachung

5 Dürfen Fotos von Mitarbeitenden im Internet veröffentlicht werden?

Ist eine Person auf einem Foto klar erkennbar, handelt es sich um Personendaten. In diesem Fall gilt, dass das Foto nur veröffentlicht werden darf, wenn die betroffene Person ihre ausdrückliche Einwilligung gegeben hat. Jede Mitarbeiterin und jeder Mitarbeiter hat das Recht, die Zustimmung

zur Publikation eines Fotos im Internet zu verweigern. Zu beachten ist, dass die betroffene Person vor der Publikation von ihrem Recht Gebrauch machen darf. Ist nämlich ein Foto einmal im Internet, besteht bereits keine Kontrolle mehr über dessen Verwendung, da es beliebig heruntergeladen, kopiert oder verändert werden kann. Obwohl es sich beim *Intranet* um einen geschützten Bereich handelt und die Gefahr einer Persönlichkeitsrechtsverletzung kleiner ist, gilt doch dasselbe auch für das Intranet. Denn auch aus dem Intranet kann ein Foto ins Internet gestellt werden. Ebenso gilt das Selbstbestimmungsrecht auch für das Intranet.

⁴ Art. 20 DSGVO.

⁵ ABIG 2008, 2321.

6 Welche Vorkehrungen im Umgang mit E-Mail sind für den Fall der Abwesenheit von Mitarbeitenden zu beachten?

Ist eine Mitarbeiterin oder ein Mitarbeiter vorhersehbar beispielsweise wegen Ferien abwesend, empfiehlt sich, den Abwesenheitsassistenten des E-Mail-Programmes zu verwenden. Darin wird über die Dauer der Abwesenheit informiert und eine Stellvertreterin oder ein Stellvertreter angegeben. Zwar besteht auch die Möglichkeit, dass die Mitarbeitenden bei Abwesenheiten im Outlook eine Stellvertretung mit abgestufter Berechtigung zur Einsicht und Weiterbearbeitung der eingehenden geschäftlichen E-Mail definieren kann. Aus datenschutzrechtlicher Sicht ist dies allerdings problematisch: Die Absenderin oder der Absender der E-Mail geht davon aus, dass ihr oder seine E-Mail einer bestimmten Person zugestellt wird. Auf eine auto-

matistische Weiterleitung hat die absendende Person keinen Einfluss. Zudem werden private E-Mail, die in der kantonalen Verwaltung in verhältnismässigem Rahmen zulässig sind, automatisch an die Stellvertreterin oder den Stellvertreter weitergeleitet, wenn die E-Mail nicht als privat gekennzeichnet ist. Als Ergänzung zur personenbezogenen E-Mail-Adresse kann sich die Schaffung einer funktionalen E-Mail-Adresse (z.B. `personalamt@sg.ch`), deren geschäftlicher Charakter sofort ersichtlich ist und die bewirtschaftet wird, als nützlich erweisen.

Bei nicht vorhersehbaren Abwesenheiten muss dem Systemadministrator von Ab-raxas der Auftrag erteilt werden, eine Abwesenheitsmeldung einzurichten.

7 **Darf die Arbeitgeberin oder der Arbeitgeber Internetgebrauch und E-Mail-Verkehr kontrollieren?**

Die Arbeitgeberin oder der Arbeitgeber darf Internetgebrauch und E-Mail-Verkehr unter folgenden drei Voraussetzungen kontrollieren:

- Arbeitgeberin oder Arbeitgeber hat ein Benutzungsreglement erlassen und dies kommuniziert.
- Das Benutzungsreglement bezeichnet die für die Kontrolle zuständige Stelle, ebenso die Bedingungen, unter denen eine personenbezogene Kontrolle zulässig ist und die allfälligen Sanktionen.
- Es wurde ein Missbrauch bzw. ein Verstoss gegen das Benutzungsreglement festgestellt oder es besteht der Verdacht auf eine Straftat.

Der Kanton St. Gallen hat die [Dienstanweisung über Einsatz und Verwendung von In-](#)

[formatikmitteln](#) erlassen. Der Dienst für Informatikplanung wurde als die für eine Kontrolle zuständige Stelle bezeichnet.

Bei einem Missbrauchsverdacht gilt folgender Meldeweg: Vorgesetzte Person – Generalsekretärin oder Generalsekretär – Sicherheitsbeauftragter des Dienstes für Informatikplanung. Wichtig ist die Führungsverantwortung der vorgesetzten Person: Vor der Auslösung des Verfahrens sollte das Gespräch mit der Mitarbeiterin oder dem Mitarbeiter gesucht werden. Diese sind auf die Dienstanweisung und die möglichen Folgen hinzuweisen.

8 **Was müssen Vorgesetzte bei einem Verdacht auf eine Straftat beachten?**

Besteht der Verdacht auf eine Straftat, darf die oder der Vorgesetzte die Personenda-

ten sicherstellen, falls die Gefahr des Verlusts besteht. Beim Kanton St. Gallen läuft das Prozedere im Fall von elektronischen Daten wie folgt ab (siehe dazu auch Punkt 7 dieser Broschüre): Die oder der Vorgesetzte der betroffenen Person wendet sich an die Generalsekretärin oder den Generalsekretär. Generalsekretärin oder Generalsekretär veranlassen beim Sicherheitsbeauftragten des Dienstes für Informatikplanung die Sicherstellung der Dokumente. Weitergehende Schritte sind danach Sache der Untersuchungsbehörden.

Mitarbeiterumfrage

9 Unter welchen Voraussetzungen darf eine Mitarbeiterumfrage durchgeführt werden?

Bei Mitarbeiterumfragen werden in der Regel besonders schützenswerte Personendaten erhoben bzw. es entstehen Persönlichkeitsprofile. Zur Durchführung braucht es daher die ausdrückliche Einwilligung der betroffenen Person. Die betroffene Person muss zudem Kenntnis von Zweck und Art der vorgesehenen Bearbeitung sowie der Freiwilligkeit der Teilnahme haben. Das öffentliche Organ muss ausserdem folgende Angaben machen: Zweck und Rechtsgrundlage der Bearbeitung, an der Beschaffung beteiligte Behörde oder Dienststelle und für diese handelnde Personen, Empfängerinnen und Empfänger der beschafften Personendaten.⁶

Zudem müssen die Personendaten anonymisiert werden, sobald es der Zweck der Bearbeitung zulässt. Bei der Bekanntgabe der Ergebnisse dürfen keine Rückschlüsse auf betroffene Personen möglich sein.⁷

10 Besteht die Pflicht zur Teilnahme an einer Mitarbeiterumfrage?

Die Arbeitgeberin oder der Arbeitgeber darf besonders schützenswerte Personendaten oder Persönlichkeitsprofile – um die es sich bei Mitarbeiterbefragungen regelmässig handelt – bearbeiten, wenn eine gesetzliche Grundlage vorhanden ist oder die Arbeitnehmerin oder der Arbeitnehmer ausdrücklich eingewilligt hat. Eine gesetzliche Grundlage gibt es im kantonalen Recht nicht. Es bedarf deshalb der ausdrücklichen Einwilligung. Eine Pflicht zur Teilnahme besteht daher nicht.

⁷

Art. 7 Abs. 1 und 2 DSG.

Verschiedenes

11 Ist es zulässig, eine Schulung mit nicht anonymisierten Personendaten durchzuführen?

Werden bei einer Schulung nicht anonymisierte Personendaten verwendet, handelt es sich um eine Bekanntgabe von – je nach Kontext – besonders schützenswerten Personendaten. Dazu braucht es eine gesetzliche Grundlage oder die ausdrückliche Einwilligung der betroffenen Person. Ansonsten ist die Verwendung nicht anonymisierter Personendaten für Schulungszwecke nicht zulässig, zumal es der Zweck der Schulung nicht erfordert.

12 Ist es zulässig, private Handy-Nummern auf einem internen Mitarbeitenden-Verzeichnis aufzuführen?

Auch wenn es sich lediglich um ein internes Verzeichnis handelt (das aber allen Mitarbeitenden verteilt wird), ist dies nur mit der ausdrücklichen Einwilligung der betroffenen Mitarbeitenden zulässig. Private Handy-Nummern sind in keinem öffentlichen Verzeichnis zu finden und dienen nicht der geschäftlichen Aufgabenerfüllung. Anders verhält es sich mit geschäftlichen Handy-Nummern: Diese dienen der geschäftlichen Aufgabenerfüllung und dürfen deshalb ohne Einwilligung auf dem Verzeichnis aufgeführt werden.

Für Fragen stehen Ihnen die Fachstelle Datenschutz (058 229 14 14) und das Personalamt (058 229 27 53) gerne zur Verfügung.

Glossar

Personendaten: Alle Angaben, die sich auf eine bestimmte oder bestimmbare Person beziehen.

Persönlichkeitsprofil: Zusammenstellung von Personendaten, welche die Beurteilung der Persönlichkeit einer natürlichen Person erlaubt.

Bearbeitung: Jeder Umgang mit Personendaten, insbesondere die Beschaffung, Aufbewahrung, Verwendung, Umarbeitung, Bekanntgabe, Archivierung, Löschung oder Vernichtung.

Bekanntgabe: Zugänglichmachen von Personendaten sowie Gewährung von Einsicht, Weitergabe und Veröffentlichung.

Öffentliches Organ: Organ, Behörde oder Dienststelle von Kanton, selbständiger öffentlich-rechtlicher Anstalt des Kantons, Gemeinde, selbständigem öffentlich-rechtlichem Gemeindeunternehmen, Gemeindeverband und Zweckverband. Dem öffentlichen Organ sind Private gleichgestellt, wenn sie Staatsaufgaben erfüllen.

Besonders schützenswerte Personendaten:

Angaben über:

1. religiöse, weltanschauliche sowie politische Ansichten und Tätigkeiten. Ausgenommen sind Angaben über die Mitgliedschaft bei einer Religionsgemeinschaft, einer Organisation oder einer politischen Partei, wenn die betroffene Person diese selbst bekannt gegeben hat oder für ein öffentliches Amt kandidiert;
2. Gesundheit, Intimsphäre und ethnische Zugehörigkeit;
3. genetische Daten;
4. biometrische Daten;

5. Leistungen und Massnahmen der sozialen Hilfe;
6. strafrechtliche sowie disziplinarische Verfahren und Sanktionen.

Grundsätze: Grundlegende Leit motive im Datenschutz, die bei allen Datenbearbeitungen zu beachten sind.

Rechtsgrundlagen und Richtlinien

- Datenschutzgesetz; sGS 142.1
- Personalgesetz, sGS 143.1
- Personalverordnung, sGS 143.11
- Richtlinie zum Umgang mit Personalunterlagen und Personaldossiers unter Einbezug der datenschutzrechtlichen und der archivrechtlichen Bestimmungen
- Dienstanweisung über den Einsatz von Informatikmitteln in der Staatsverwaltung

Grundsätze

Gesetzmässigkeit: Alle Datenbearbeitungen müssen auf einem Rechtssatz (Verfassung, Gesetz, Verordnung) beruhen.

Verhältnismässigkeit: Datenbearbeitungen müssen geeignet und erforderlich sein um das definierte Ziel zu erreichen. Zudem müssen das angestrebte Ziel und der Eingriff, den die Datenbearbeitung bei der betroffenen Person bewirkt, in einem vernünftigen Verhältnis zueinanderstehen.

Zweckmässigkeit: Personendaten dürfen nur für den in der Rechtsgrundlage festgelegten Zweck oder den Zweck, der bei der Beschaffung angegeben wurde oder der aus den Umständen ersichtlich ist, bearbeitet werden.

Treu und Glauben: Gebot eines loyalen und vertrauenswürdigen Verhaltens im Rechtsverkehr.

Transparenz: Beschaffung und Zweck müssen für die betroffene Person erkennbar sein.

Aktualität und Richtigkeit: Die Daten müssen aktuell und richtig sein.

Datensicherheit: Das öffentliche Organ trifft organisatorische und technische Massnahmen zur Sicherung der Daten vor Verlust und Entwendung sowie unbefugter Kenntnisnahme und unbefugtem Bearbeiten.

Datenvermeidung: Grundsatz, dass Personendaten nur dann bearbeitet werden, wenn dies notwendig ist. Ansonsten sollen anonymisierte Daten verwendet werden.

Datensparsamkeit: Grundsatz, dass nur diejenigen Personendaten bearbeitet werden, die für die Aufgabenerfüllung auch wirklich benötigt werden ("so wenig wie möglich, nur so viel wie nötig").