Datenschutzhandbuch

forwerts interactive GmbH

Friedensstrasse 11

60311 Frankfurt

Inhalt

1. Ziel

Dieses Dokument enthält die wesentlichen Prozesse, die für den Umgang mit personenbezogenen Daten zu beachten sind. Hiermit soll jedem Mitarbeiter die Möglichkeit gegeben werden, die Prozesse zur Datenschutz-Grundverordnung nachvollziehen zu können. Hierdurch sollen zudem eine einheitliche Abwicklung sowie überprüfbare Handhabung und Dokumentation gewährleistet werden.

Ziel dieses Datenschutzhandbuchs ist es, die Rechtsvorschriften für die Wahrung der Rechte der betroffenen Personen einzuhalten. Das Datenschutzhandbuch ist in der aktuellen Fassung für alle Mitarbeiter verbindlich. Hier werden ebenfalls die zugehörigen Grundlagen der Datenschutz-Grundverordnung erläutert, als auch die internen und externen Meldewege beschrieben. Dieses Dokument wird um die notwendigen Arbeitspapiere ergänzt und gilt als umfängliche Arbeitsanweisung.

2. Datenschutzbeauftragter

Die forwerts interactive GmbH hat einen Datenschutzbeauftragten benannt. Der Datenschutzbeauftragter ist Ansprechpartner für die Themen zum Datenschutz im Unternehmen. Er berät, kontrolliert und unterstützt die Unternehmensleitung und Mitarbeiter bezüglich der Datenverarbeitung im Unternehmen.

Im Bereich der Verarbeitung von personenbezogenen Daten ist Sorge dafür zu tragen, dass eine frühe Einbindung des Datenschutzbeauftragten bei der Planung und Einführung von neuen Prozessen, in deren Zusammenhang auch personenbezogene Daten verarbeitet werden, erfolgt.

Kontaktdaten des Datenschutzbeauftragten:

KLW GmbH
Herr Wolfgang Matzke
Edisonstraße 23
74076 Heilbronn
datenschutz@klw.de

3. Definition

Bei personenbezogenen Daten handelt es sich um alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen. Man spricht hierbei im Datenschutz von der „betroffenen Person“. Eine betroffene Person ist identifizierbar, wenn direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind, identifiziert werden kann (Art. 4 Abs. 1 DSGVO).

Besonders sensible personenbezogene Daten sind nach Art. 9 DSGVO solche aus denen die rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, sowie genetischen Daten, biometrischen Daten zur eindeutigen Identifizierung einer natürlichen Person, Gesundheitsdaten oder Daten zum Sexualleben oder der sexuellen Orientierung einer natürlichen Person. Diese personenbezogenen Daten unterliegen noch strengeren Voraussetzungen zur Datenverarbeitung und sind aus diesem Grund besonders schützenswert.

Der Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten ist ein Grundrecht. Jede Person hat gemäß der Charta der Grundrechte der Europäischen Union das Recht auf Schutz der sie betreffenden personenbezogenen Daten. Daher sollen die Vorschriften zum Schutz natürlicher Personen bei der Verarbeitung ihrer personenbezogenen Daten gewährleisten, dass deren Grundrechte und Grundfreiheiten gewahrt werden.

4. Datenschutzgrundsätze zur Verarbeitung von personenbezogenen Daten

Die Grundsätze der Verarbeitung von personenbezogenen Daten sind in Art. 5 der Datenschutzgrundverordnung definiert. Sie sind für die Verarbeitung verbindlich, und müssen daher bei der Verarbeitung personenbezogener Daten eingehalten werden, und gemäß Art. 5 Abs. 2 DSGVO nachgewiesen werden können.

4.1 Rechtmäßigkeit

Der Grundsatz der Rechtmäßigkeit besagt, dass eine Verarbeitung von personenbezogenen Daten nur dann erlaubt ist, wenn es hierfür einen Erlaubnistatbestand, die vorwiegend in den Art. 6 und 9 der DSGVO bestimmt sind, gibt. Eine Rechtsgrundlage kann insbesondere ein Vertrag mit der betroffenen Person, ein berechtigtes Interesse des Unternehmens unter Abwägung des Interesses und der Grundrechte und Grundfreiheiten der betroffenen Personen oder eine Einwilligung sein.

Die Einwilligung gilt nicht als freiwillig erteilt, wenn zu verschiedenen Verarbeitungsvorgängen von personenbezogenen Daten nicht gesondert eine Einwilligung erteilt werden kann, obwohl dies im Einzelfall angebracht ist, oder wenn die Erfüllung eines Vertrags, einschließlich der Erbringung einer Dienstleistung, von der Einwilligung abhängig ist, obwohl diese Einwilligung für die Erfüllung nicht erforderlich ist.

4.2 Verarbeitung nach Treu und Glauben

Hierbei sind insbesondere die Informationspflichten und die Rechte der Betroffenen in nachvollziehbarer Weise zu erfüllen. Dabei muss die Datenverarbeitung unter Berücksichtigung der Interessen der betroffenen Personen im Hinblick auf ihre Grundrechte angemessen sein.

4.3 Transparenz

Der Grundsatz der Transparenz fordert, dass jeder Betroffene wissen soll, wer welche Daten für welche Zwecke über ihn erhebt, verarbeitet, speichert und übermittelt und wie lange diese Daten gespeichert sind. Diese Daten müssen in klarer und einfacher Sprache abgefasst und leicht zugänglich und verständlich sein. Natürliche Personen sind über die Risiken, Vorschriften, Garantien und Rechte im Zusammenhang mit der Verarbeitung personenbezogener Daten zu informieren und darüber aufzuklären, wie sie ihre diesbezüglichen Rechte geltend machen können. Die Informationen müssen einfach und verständlich sein.

4.4 Zweckbindung

Der Grundsatz der Zweckbindung besagt, dass personenbezogene Daten nur für eindeutig festgelegte und legitime Zwecke erhoben werden dürfen. Eine Weiterverarbeitung, die nicht mit den vorab festgelegten Zwecken vereinbar ist, ist dadurch verboten. Eine Verarbeitung oder Nutzung von personenbezogenen Daten für andere als den Betroffenen im Zusammenhang mit der Datenerhebung kommunizierten Zwecke ist nur unter den gesetzlich festgelegten Bedingungen (Art. 6 Abs. 4 DSGVO) und ansonsten nur mit Einwilligung der Betroffenen zulässig.

4.5 Datenminimierung

Der Grundsatz der Datenminimierung (Art. 5 Abs. 1 lit. c) DSGVO) besagt, dass eine Verarbeitung von personenbezogenen Daten dem Zweck angemessen und auf das notwendigste Mindestmaß, das für die Zwecke der Verarbeitung benötigt wird, beschränkt. Es dürfen nur solche Daten erhoben werden, die wirklich erforderlich sind und diese Daten dürfen nur so lange gespeichert werden, wie sie tatsächlich benötigt werden. Darüberhinausgehende Erhebungen und Verarbeitungen sind unzulässig.

4.6 Richtigkeit

Im Hinblick auf die Zwecke ihrer Verarbeitung müssen die personenbezogenen Daten nach Art. 5 Abs. 1 d) DSGVO sachlich richtig und erforderlichenfalls auf dem neuesten Stand sein. Die Verarbeitung unrichtiger Daten gilt es zu vermeiden. Zur Berichtigung oder Löschung unrichtiger Daten sind alle angemessenen Maßnahmen zu treffen.

4.7 Speicherbegrenzung & Löschung

Personenbezogene Daten dürfen nur so lange gespeichert werden, wie es für die Zwecke, für die Sie erforderlich sind, notwendig ist, wenn dem keine gesetzliche Aufbewahrungsfrist entgegenstehen. Personenbezogene Daten, die nicht mehr für die Zwecke, für die sie erhoben wurden, notwendig sind, müssen daher regelmäßig gelöscht werden.

4.8 Integrität und Vertraulichkeit

Personenbezogene Daten müssen in einer Weise verarbeitet werden, die eine angemessene Sicherheit gewährleistet, einschließlich Schutz vor unbefugter oder unrechtmäßiger Verarbeitung und vor unbeabsichtigtem Verlust, Zerstörung oder Schädigung durch geeignete technische und organisatorische Maßnahmen (Art. 5 Abs. 1 f) DSGVO).

5. Datenschutz-Pflichtdokumentation

5.1 Verarbeitungsverzeichnisse

Der Verantwortliche und der Auftragsverarbeiter sind zur Führung eines Verzeichnisses der Verarbeitungstätigkeit gemäß Art. 30 der Datenschutz-Grundverordnung verpflichtet. Der Verantwortliche legt darin u. a. die Kategorien von betroffenen Personen, Kategorien von Daten und die Empfänger im Verarbeitungsprozess offen. Der Auftragsverarbeiter führt u. a. die Verantwortlichen, für die er tätig ist, und die jeweils vereinbarten Dienstleistungen auf.

Die forwerts interactive GmbH führt ein Verzeichnis von Verarbeitungstätigkeiten, welches von der der IT , geführt wird. Die IT trägt dafür Sorge, dass die Verarbeitungsverzeichnisse regelmäßig aktualisiert werden.

Alle Beschäftigten, die für die Einrichtung oder Durchführung von Verarbeitungstätigkeiten verantwortlich sind, sind bei einer geplanten Einrichtung oder Änderung von Verarbeitungen und/oder Geschäftsprozessen verpflichtet, dieses der der IT mitzuteilen.

5.2 Auftragsdatenverarbeitungen

Werden personenbezogene Daten im Auftrag einer verantwortlichen Stelle durch andere Personen oder Stellen verarbeitet, bleibt die auftraggebende Stelle für die Einhaltung der Bestimmungen dieses Gesetzes und anderer Vorschriften über den Datenschutz verantwortlich.

Ein Auftragsverarbeitungsvertrag wird nötig, wenn personenbezogene Daten im Auftrag an Dritte weitergegeben und von ihnen verarbeitet oder genutzt werden. Die rechtlichen Vorschriften zur Datenverarbeitung durch einen Auftragsverarbeiter sind in Art. 28 DSGVO festgelegt.

Ein Auftragsverarbeitungsvertrag muss immer vor Verarbeitung durch einen Auftragsverarbeiter abgeschlossen werden. Hierbei ist auch auf die durch den Auftragsverarbeiter getroffenen technischen und organisatorischen Maßnahmen zu achten, da der Verantwortliche sicherstellen muss, dass personenbezogene Daten bei den zur Verarbeitung eingesetzten Auftragnehmern, ebenfalls gemäß den Vorschriften der DSGVO behandelt werden.

Alle Beschäftigten, die für die Hinzuziehung neuer Lieferanten bzw. Dienstleister verantwortlich oder in diesem Geschäftsprozess involviert sind, in denen eine Verarbeitung von personenbezogenen Daten vorkommt, sind dazu verpflichtet diese Verarbeitung der IT mitzuteilen, um eine Prüfung zur Notwendigkeit eines Auftragsdatenverarbeitungsvertrags einleiten zu können, sodass die vorherige Prüfung hinsichtlich eines AV-Vertrags im Sinne der Datenschutz-Grundverordnung durchgeführt werden kann. Die Prüfung über die Notwendigkeit eines solchen Vertrags führt der Datenschutzbeauftragter durch. Alle Beschäftigten sind verpflichtet, diesen Meldeweg durchzuführen, wenn personenbezogene Daten im Auftrag verarbeitet werden, insbesondere, da die Datenweitergabe und die Datenverarbeitung durch einen Auftragsverarbeiter ohne entsprechenden Abschluss eines Auftragsdatenverarbeitungsvertrags ein Bußgeld nach sich ziehen kann.

6. Rechte der betroffenen Person

Jede natürliche Person (z.B. Mitarbeiter, Bewerber oder Kunden) hat nach der DSGVO das Recht, über die zu seiner Person erhobenen Daten, selbst zu bestimmen. Diese Rechte sind unabdingbar, d.h. diese können nicht eingeschränkt oder durch Einwilligung entkräftet werden.

Die in der DSGVO in den Art. 12 ff. DSGVO aufgezählten Betroffenenrechte stellen somit ein Steuerungs- und Kontrollelement hinsichtlich der Verarbeitung personenbezogener Daten dar. Das sind Rechte, die dem Betroffenen Mitwirkungsmöglichkeiten und Einwirkungsmöglichkeiten auf die Verarbeitung ihn betreffender personenbezogener Daten gewähren.

Folgende Rechte stehen dem Betroffenen im Rahmen seiner Datenverarbeitung zu:

1. Recht auf Auskunft (Art. 15 DSGVO)
2. Recht auf Berichtigung (Art. 16 DSGVO)
3. Recht auf Löschung (Art. 17 DSGVO)
4. Recht auf Einschränkung (Art. 18 DSGVO)
5. Recht auf Datenübertragbarkeit (Art. 20 DSGVO)
6. Recht auf Widerspruch (Art. 21 DSGVO)
7. Beschwerderecht bei der Aufsichtsbehörde (Art. 77 DSGVO i. V. m. § 19 BDSG).

6.1 Umgang mit Betroffenenrechten / Regelung zum Auskunftsverlangen

Werden Betroffenenrechte geltend gemacht, muss der Verantwortliche bestimmte formale Voraussetzungen beim Umgang mit diesen Rechten beachten.

Die Betroffenenanfrage muss **innerhalb eines (1) Monats** nach Eingang der Anfrage gegenüber dem Betroffenen beantwortet werden. Danach hat der Betroffene das Recht sich mit seinem Auskunftsersuchen an die Aufsichtsbehörde zu wenden.

Im Einzelfall kann eine Verlängerung erfolgen, diese ist zu begründen, dem Betroffenen vorab mitzuteilen und entsprechend zu dokumentieren.

Der Betroffene kann seine Rechte grundsätzlich formlos, dies bedeutet schriftlich oder mündlich geltend machen.

6.2 Interne Vorgehensweise

Die Geschäftsleitung sowie die IT ist über alle eingehenden Anfragen zum Betroffenenrecht umgehend in Kenntnis zu setzen.

Die IT erfüllt folgende Aufgaben:

- Sichtung der Anfragen
- Erstdokumentation (hierzu wird das Dokument „**Checkliste-Dokumentation_Betroffenenanfrage_forwerts interactive GmbH“** verwendet)
- Interne und externe Kommunikation, sowie Terminüberwachung
  die Überwachung und Zusammenstellung der erforderlichen Informationen, die im Haus gesammelt werden, obliegt der IT.
- Ggf. Prüfung des Mitarbeiterstatus, wenn es sich um einen (ehemaligen) Mitarbeiter handelt
- Information des Datenschutzbeauftragten, Absprache des weiteren Vorgehens
- Sowie mit dem/durch den Datenschutzbeauftragten geklärt ist, in welchem Rahmen das Auskunftsersuchen liegt, werden die Fachabteilungen durch die beauftragte Stelle informiert und mit der Zusammenstellung beginnen.
  Im Zweifel geht die Anfrage an alle Fachabteilungen.
- Es ist zwingend notwendig, dass die angefragte Fachabteilung die Anfrage unverzüglich bearbeitet, da die Bearbeitung von Betroffenenrechte innerhalb einer kurzen Frist zu erfolgen hat und bei Nichtbeachtung hohe Bußgelder drohen.

6.3 Feststellung der Identität

Soweit die Identität nicht intern durch Einsichtnahme eines Ausweisdokumentes vor Ort vorgenommen wurde, nimmt der Datenschutzbeauftragte Kontakt mit dem Betroffenen auf, wobei hierbei die Wünsche des Betroffenen soweit möglich berücksichtigt werden.

So wird der potenziell Betroffene nur angerufen oder per E-Mail kontaktiert, wenn er damit einverstanden ist.

Bestehen Zweifel an der Identität, wird der Schriftverkehr über die Postanschrift mittels Post-Ident abgewickelt.

6.4 Feststellung der Berechtigung, Art, Umfang und Vorgehen

Nach Mitteilung gilt es festzustellen und zu prüfen, ob es sich um ein Verlangen nach den Bestimmungen der DSGVO und im Sinne des Datenschutzrechtes handelt.

Soweit der Datenschutzbeauftragte mit dem Betroffenen die Anfrage geklärt hat, wird er die IT darüber informieren, die in Folge die notwendige Datensammlung koordiniert.

Der Antragsteller erhält eine Eingangsbestätigung und weiß damit, dass seine Anfrage behandelt wird und in welchem Zeitrahmen mit der Erledigung zu rechnen ist.

7. Datenpannen („Data Breach“) / Datenschutzverletzung

7.1 Definition Datenpanne/Datenschutzverletzung

Die Definition einer Datenschutzverletzung lautet gem. Art. 4 Nr. 12 DSGVO wie folgt: Eine Verletzung des Schutzes personenbezogener Daten („Datenschutzverletzung“) liegt bei jeder Verletzung der Datensicherheit vor, die zur Vernichtung, zum Verlust oder zur Veränderung, ob unbeabsichtigt oder unrechtmäßig oder zur unbefugten Offenlegung von beziehungsweise zum unbefugten Zugang zu personenbezogenen Daten führt, die übermittelt, gespeichert oder auf sonstige Weise verarbeitet wurden.

Beispiele einer Datenschutzverletzung:

- Verlust oder Diebstahl eines Notebooks, Tablet-PCs, USB-Sticks, einer Daten-CD-ROM oder eines anderen, zumal unverschlüsselten, mobilen Speichergeräts
- Hackerangriffe, sowie rechtswidrige Datenübermittlungen wie bspw. auch der Weiterverkauf von Daten durch Mitarbeiter
- Unsachgemäße Entsorgung von Dokumenten und Informationen in analoger, sowie digitaler Form und Altgeräten, z. B. Computern, Festplatten, etc.
- Übermittlung von Daten an falsche Empfänger (hierzu zählen auch fehlgeleitete E-Mails)

7.2 Meldepflicht Aufsichtsbehörde

Liegt eine Verletzung des Schutzes personenbezogener Daten vor, muss dieses der Aufsichtsbehörde innerhalb von **72 Std**. gemeldet werden.

Seit dem 25. Mai 2018 ist mit Inkrafttreten der Datenschutz-Grundverordnung (DSGVO) auch eine abgestufte Meldepflicht bei Datenpannen, also Verletzungen des Schutzes personenbezogener Daten, vorhanden.

Die Meldung an die zuständige Aufsichtsbehörde hat innerhalb von **72 Stunden** nach Kenntniserlangung (auch an Wochenenden, Feiertagen, sowie sonstigen Betriebsschließungen) zu erfolgen.

Die Beurteilung erfolgt durch den Datenschutzbeauftragten.

7.3 Interner Meldeweg

Wenn eine mögliche Datenschutzverletzung festgestellt wird, ist es von besonderer Bedeutung, dass sofort agiert wird. Um eine Meldung der möglichen Datenpanne innerhalb der rechtlich vorgegebenen Frist von 72 Stunden durchführen zu können, wurde folgender Ablaufplan erstellt.

- Erstdokumentation

- Die Geschäftsleitung und die IT sind sofort zu informieren, um den Vorgang intern zu prüfen und weiteren Schaden abzuwenden. Darüber hinaus wird die Datenschutzverletzung dokumentiert (hierzu wird das Dokument **„Checkliste-Dokumentation Datenschutzverletzungen_forwerts interactive GmbH“** verwendet)

- Nach Feststellung der betroffenen Daten, bzw. wenn ersichtlich wird, dass eine Datenschutzverletzung besteht und welche Kategorien betroffen sind, wird der Datenschutzbeauftragte unverzüglich hinzugezogen und ggf. eine Meldung an die Datenschutz Aufsichtbehörde durchgeführt.

7.4 Mitteilungspflicht an Betroffene

Unter Umständen müssen in Folge der Datenschutzverletzung die Betroffenen über Art und Umfang der Datenschutzverletzung in Kenntnis gesetzt werden. Dies ist dann der Fall, wenn voraussichtlich ein hohes Risiko für die Rechte und Grundfreiheiten der vom Datenschutzvorfall betroffenen Personen besteht. Die Einschätzung über eine Benachrichtigungspflicht erfolgt in Zusammenarbeit mit dem Datenschutzbeauftragten.