Unternehmens-Richtlinien

Prozess Datenschutz Compliance

Datenschutz-Richtlinie

Druck+Verlag Ernst Vögel GmbH
Binderei und Versand Ernst Vögel GmbH
Vögel GmbH & Co. KG
VOB-Verlag Vögel OHG

Kalvarienbergstraße 22
93491 Stamsried

vorgelegt von

atarax Unternehmensgruppe

Luitpold-Maier-Str. 7
D-91074 Herzogenaurach

Bearbeiter:
Jackwirth

Version 1.0
10/2024

Rechtsgebiete
Auch wenn es Überschneidungen mit anderen Rechtsgebieten, wie z.B. Zivil-, Wettbewerbs-, Arbeits- oder Betriebsverfassungsrecht gibt, bitten wir um Ihr Verständnis, dass wir uns aus rechtlichen Gründen auf datenschutzrechtliche Belange beschränken.

Geschlechtsneutrale Formulierung
Ausschließlich zum Zweck der besseren Lesbarkeit wird auf die geschlechtsspezifische Schreibweise verzichtet. Alle personenbezogenen Bezeichnungen in diesem Dokument sind somit geschlechtsneutral zu verstehen.

Änderungshistorie

Version	Datum	Bearbeiter	Kapitel	Änderung

1 Vorbemerkung

Der Schutz personenbezogener Daten ist uns ein wichtiges Anliegen. Deshalb verarbeiten wir die personenbezogenen Daten unserer Mitarbeiter, Kunden, Lieferanten sowie anderer Geschäftspartner in Übereinstimmung mit den anwendbaren Rechtsvorschriften zum Schutz personenbezogener Daten und zur Datensicherheit. Die maßgeblichen Regelungen zum Thema Datenschutz sind in der Datenschutz-Grundverordnung (DS-GVO) sowie in den entsprechenden Ausführungsgesetzen (in Deutschland z. B. im Datenschutz-Anpassungs- und Umsetzungsgesetz, kurz: „BDSG-neu“) enthalten. Alle Vorschriften haben dasselbe Ziel, die Persönlichkeitsrechte und die Privatsphäre jedes Menschen zu schützen.

2 Datenschutz und Persönlichkeitsrecht

2.1 Leitgedanke und Ziele

Durch die Richtlinie soll ein einheitlicher Standard für den Schutz personenbezogener Daten geschaffen werden. Dem erklärten Unternehmensziel, sowohl die Persönlichkeitsrechte der Mitarbeiter, Kunden, Lieferanten als auch der anderen Geschäftspartner zu schützen, wird durch die Schaffung eines angemessenen und rechtskonformen Datenschutzniveaus im Sinne der DS-GVO entsprochen.
Die ordnungsgemäße Datenverarbeitung sowie eine wirksame und effektive Datenschutzorganisation sind zentrale Voraussetzungen für die Erfüllung unserer Unternehmensziele.

Zudem haben Unternehmen aufgrund der umgekehrten Beweislast eine sogenannte „Rechenschaftspflicht“. Das bedeutet, dass bei einer etwaigen Datenschutzprüfung unsere Unternehmen nachweisen müssen, dass wir datenschutzkonform arbeiten. Daher müssen unternehmensweit geltende Richtlinien wie diese sowie die wichtigen Datenschutzprozesse dokumentiert und auch regelmäßig auf ihre Wirksamkeit hin geprüft werden.

In Anbetracht der hohen Bußgelder von zwei bis vier Prozent des weltweiten jährlichen Jahresumsatzes oder 10 bzw. 20 Mio. Euro (der jeweils höhere Betrag gilt) ist dies elementar für unsere Unternehmen. Schadensfälle oder ein Imageschaden müssen verhindert werden.

Die Selbstverantwortung des einzelnen Mitarbeiters in seinem jeweiligen Arbeitsbereich und das Erkennen, dass ein gelebter Datenschutz ein wesentliches Element unserer Unternehmensphilosophie ist, sind besonders wichtig. Von jedem Mitarbeiter wird ein stets vorhandenes Bewusstsein im Bereich Datenschutz bei allen täglich anfallenden Tätigkeiten erwartet.

2.2 Anwendungsbereich

Diese Richtlinie gilt für alle Mitarbeiter der Druck+Verlag Ernst Vögel GmbH, der Binderei und Versand Ernst Vögel GmbH, der Vögel GmbH & Co. KG und der VOB-Verlag Vögel OHG (im Folgenden „die Unternehmen“), die mit personenbezogenen Daten umgehen.

2.3 Verantwortung und Umsetzung

2.3.1 Unternehmensleitung

Die Unternehmensleitung ist als Stelle, die über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet oder eine Datenverarbeitung im Auftrag vornehmen lässt, als „Herr über die Daten“ für diese verantwortlich. Sie hat die Verantwortung, dass der gesetzlich erforderliche Datenschutz sowie die relevanten Datenschutzprozesse umgesetzt und auch durch Installation ausreichender Kontrollmechanismen regelmäßig überwacht werden.

Die Unternehmen haben außerdem ein Verzeichnis über alle Verarbeitungsvorgänge (kurz: „VVT“), bei denen personenbezogene Daten betroffen sind, zu führen. In jeder Fachabteilung (sogenannte „Dateneigner“) wird mindestens einer Person die Verantwortung übertragen, die dafür notwendigen Informationen zu den Verfahren der jeweiligen Abteilung zusammenzutragen und diese entsprechend den Anforderungen des Art. 30 DS-GVO zu dokumentieren. Zudem muss bei Vorliegen der Voraussetzungen eine sogenannte „Datenschutz-Folgenabschätzung“ gem. Art. 35 DS-GVO durchgeführt werden. Die diesbezüglichen Prozesse werden in der Anlage der Datenschutz-Richtlinie ausführlich dargestellt.

Bei Unklarheiten hinsichtlich der gesetzlich geforderten Informationen kann der Datenschutzbeauftragte selbstverständlich beratend hinzugezogen werden. Auf Anfrage stellen die Unternehmen der Aufsichtsbehörde das Verzeichnis zur Verfügung. Im Einvernehmen mit der Unternehmensleitung ist hierfür der Datenschutzbeauftragte zuständig und arbeitet mit der Aufsichtsbehörde zusammen.

2.3.2 Fachverantwortliche / Führungskräfte

Datenschutz ist ein integraler Bestandteil der originären Fachaufgabe. Damit trägt jede Führungskraft die Verantwortung zur Sicherstellung des Datenschutzes in ihrem Aufgabenbereich. Jeder Vorgesetzte ist verpflichtet, die Einhaltung der Vorschriften zum Datenschutz durch seine Mitarbeiter sicherzustellen und auch regelmäßig zu kontrollieren. Jeder Mitarbeiter, der Schwachstellen im Bereich der Datensicherheit oder des Datenschutzes erkennt, ist verpflichtet, diese seinem Vorgesetzten zu melden.

2.3.3 Datenschutzbeauftragter

Die Unternehmen haben die atarax Unternehmensgruppe als Datenschutzbeauftragten bestellt. Dieser übernimmt die kraft Gesetzes festgelegten Aufgaben und berät die Unternehmensleitung sowie Mitarbeiter hinsichtlich der Datenschutzthemen. Der Datenschutzbeauftragte legt mit der Geschäftsleitung das strategische Vorgehen zum Datenschutz fest und unterstützt diese.

Ihm obliegt ferner die Kontrolle der Einhaltung der Datenschutzvorschriften. Er berichtet unmittelbar der Unternehmensleitung. Der Datenschutzbeauftragte ist der Unternehmensleitung direkt unterstellt und agiert gemäß den gesetzlichen Bestimmungen weisungsfrei. Dies ist im Organigramm entsprechend vermerkt.

Sie können sich bei Fragen und Problemen zum Thema Datenschutz jederzeit an **datenschutz@voegel.com** wenden.

3 Grundsätze und Begriffe

3.1 Personenbezogene Daten / Sensible Daten

Von der DS-GVO werden sogenannte „personenbezogene Daten“ geschützt.

Personenbezogene Daten sind alle Informationen, mit denen man die Person identifizieren kann. Geschützt ist dabei nur die natürliche Person, also ein Mensch. Die juristische Person als solche, z. B. die Druck+Verlag Ernst Vögel GmbH samt Firmenanschrift unterliegt nicht dem Anwendungsbereich der DS-GVO. Sobald aber ein Ansprechpartner oder eine E-Mail-Adresse, bestehend aus Vor- und Nachname, vorliegt, ist ein Personenbezug gegeben. Für den Personenbezug reicht es auch schon aus, wenn die natürliche Person identifizierbar ist, also anhand anderer Merkmale bestimmt werden kann. Im Zeitalter der Digitalisierung ist auch an die Identifizierung der Person mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten oder zu einer Online-Kennung zu denken.

Beispiele für personenbezogene Daten sind:

- Kontaktdaten (Name, E-Mail-Adresse, Anschrift, Telefonnummer), Familienstand, Geburtsdatum, Beruf, Schulbildung, Fähigkeitsprofil sowie Aussehen
- Daten, die einen Sachverhalt bezeichnen, der mit einer Person verbunden ist, wie z. B. Grundbesitz oder Vermögen

Beispiele für personenbeziehbare Daten sind:

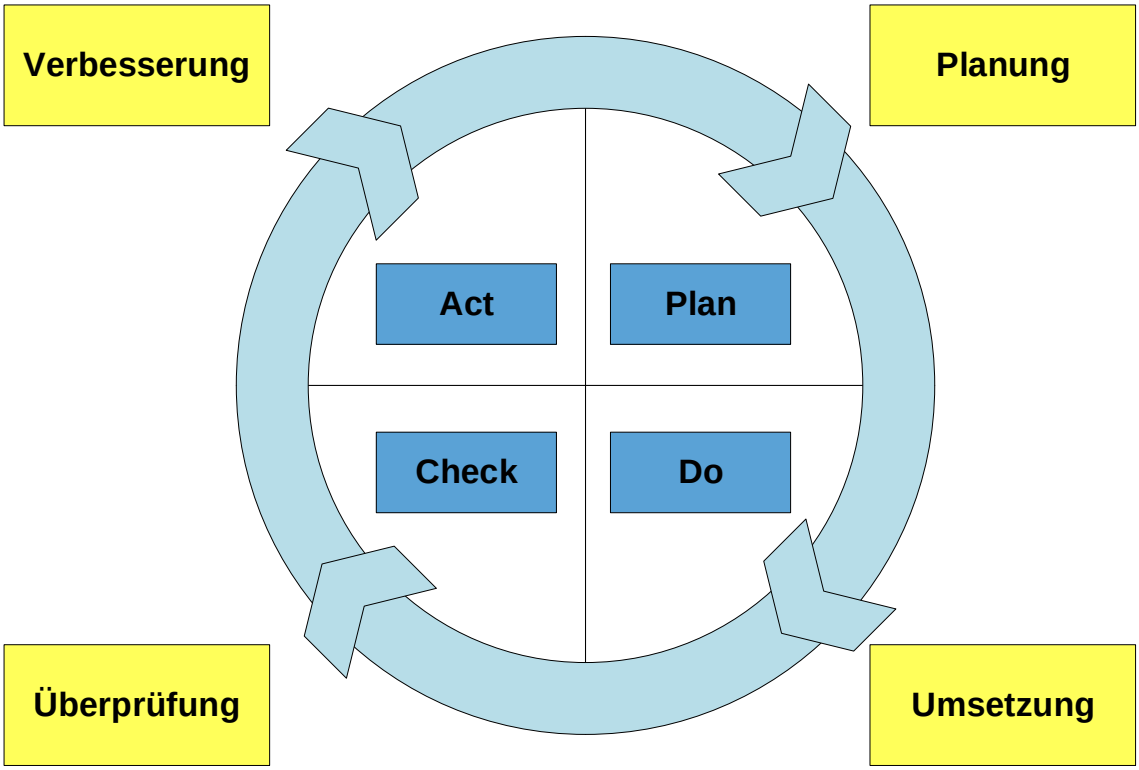
- KFZ-Kennzeichen des Autos
- IMEI-Nummer, IP-Adresse

Sämtliche personenbezogenen Daten werden von der DS-GVO geschützt.
Art. 9 DS-GVO zählt jedoch sogenannte „besondere Kategorien von personenbezogenen Daten“ auf. Diese Daten unterliegen aufgrund ihrer besonderen Sensibilität nochmal einem strengeren Schutz und die Verarbeitung ist nur unter restriktiven Vorgaben zulässig. Hierzu zählen:

Rassische und ethnische Herkunft, politische Meinung, religiöse oder weltanschauliche Überzeugung, Gewerkschaftszugehörigkeit, Gesundheitsdaten sowie genetische und biometrische Daten und Daten zum Sexualleben oder der sexuellen Orientierung.

3.2 Rechenschaftspflicht

Die Unternehmen trifft, wie bereits erwähnt, eine Rechenschaftspflicht nach Art. 5 DS-GVO (sogenannte „Accountability“). Dies bedeutet, dass unsere Unternehmen bei etwaigen Prüfungen der Datenschutzaufsichtsbehörde in der Nachweispflicht sind, sogenannte „umgekehrte Beweislast“. Wir müssen daher nachweisen, dass wir die im Folgenden näher erläuterten Grundsätze bei der Datenverarbeitung beachten. Aufgrund der Nachweispflicht ist daher ein wirksames und nachweisbares Datenschutzmanagement für die Unternehmensverteidigung elementar.



3.3 Rechtmäßigkeit der Verarbeitung / Verarbeitung nach Treu und Glauben / Transparenz

Bei der Verarbeitung personenbezogener Daten müssen die Persönlichkeitsrechte der betroffenen Personen gewahrt werden. Daher müssen die Daten auf rechtmäßige Weise, nach Treu und Glauben und in einer für die betroffene Person nachvollziehbaren Weise, also transparent, verarbeitet werden.

Die Verarbeitung von personenbezogenen Daten bzw. eine Datenübermittlung darf nur im Rahmen des rechtlich Zulässigen erfolgen. Jede Datenverarbeitung muss durch eine Rechtsgrundlage legitimiert sein (sogenanntes „Verbot mit Erlaubnisvorbehalt“).

3.4 Datenminimierung

Jede Verarbeitung von Daten durch Personen oder durch Informations- und Kommunikationssysteme muss so angelegt sein, dass so wenige Daten wie möglich erhoben werden. Hintergrund ist, dass die Datenschutz-Grundverordnung dies vorschreibt. Es dürfen also in unseren Unternehmen nur die Daten verarbeitet werden, die zwingend für die Aufgabenerfüllung bzw. den verfolgten Zweck benötigen werden.

3.5 Zweckbindung der Datenverarbeitung

Vor der Verarbeitung der personenbezogenen Daten muss ein legitimer Verwendungszweck festgelegt und in das Verarbeitungsverzeichnis (VVT) aufgenommen werden. Es muss zudem nachweislich sichergestellt werden, dass die Zweckbindung in den Unternehmen eingehalten wird. Nachträgliche Zweckänderungen sind nur unter engen Voraussetzungen möglich und müssen dokumentiert werden. Um den Nachweis für die Einhaltung des Grundsatzes der Zweckbindung führen zu können, ist daher das VVT für die Unternehmen elementar.

3.6 Datenqualität

Die erhobenen Daten müssen sachlich richtig und aktuell sein. Es müssen alle angemessenen Maßnahmen getroffen werden, damit personenbezogene Daten im Hinblick auf den Verarbeitungszweck berichtigt werden.

3.7 Speicherbegrenzung

Die Grundsätze der Datenverarbeitung personenbezogener Daten der DS-GVO schreiben die Löschung personenbezogener Daten vor, sobald der definierte Zweck für die Datenverarbeitung entfallen ist. Diese Anforderung steht primär im Spannungsverhältnis zu rechtlichen Aufbewahrungspflichten. Vereinfacht lässt sich Folgendes festhalten:

- Personenbezogene Daten sind zu löschen, sobald diese im Verfahren (datenschutzrechtlicher Prozess) nicht mehr benötigt werden,
- es keine gesetzliche Aufbewahrungspflicht gibt und
- es auch keine rechtlichen Aufbewahrungsgründe (bspw. zivilrechtlich vereinbarte Aufbewahrungszeiten, Aufbewahrungsgründe zur Erfüllung / Nachvollziehbarkeit von Rentenansprüchen oder Aufbewahrungsgründe zur Abwehr zivilrechtlicher Klagen etc.) gibt.

Die Unternehmen haben zur Erfüllung dieser rechtlichen Anforderung ein individuelles Löschkonzept, angelehnt an die DIN 66398, etabliert. Bei Fragen zur Umsetzung und Löschung der Daten wenden Sie sich bitte an Frau Barbara Bucher.

3.8 Datensicherheit / Vertraulichkeit

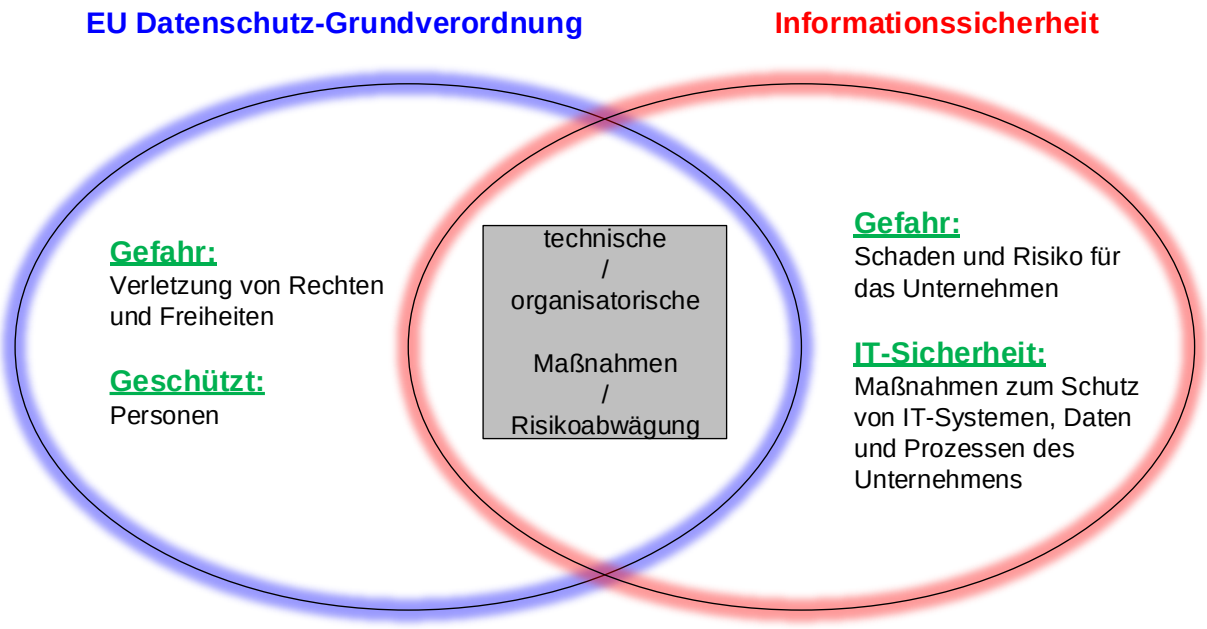


Abbildung: Gemeinsamkeiten von Datenschutz und IT-Sicherheit

Personenbezogene Daten müssen so verarbeitet werden, dass eine angemessene Datensicherheit gewährleistet wird. Die Daten müssen jederzeit gegen unbefugten Zugriff, unrechtmäßige Verarbeitung oder Weitergabe sowie gegen Verlust, Zerstörung oder Schädigung durch geeignete technische und organisatorische Maßnahmen geschützt werden. Dies gilt unabhängig davon, ob die Datenverarbeitung elektronisch oder in Papierform erfolgt.

Die Sicherheitsmaßnahmen müssen also sowohl die Wahrung der Verfügbarkeit, Vertraulichkeit und Integrität der Daten als auch die Belastbarkeit der Systeme sicherstellen.

Die DS-GVO schreibt vor, dass die Sicherheitsmaßnahmen anhand einer risikoorientierten Betrachtungsweise und unter Berücksichtigung des Standes der Technik sowie der Implementierungskosten zu treffen sind. Daher müssen Risikoanalysen für die Datenverarbeitungsprozesse durch die Fachabteilung in Zusammenarbeit mit der IT-Abteilung durchgeführt und dokumentiert werden. Die Risikoanalyse erfolgt dabei aus Sicht der betroffenen Person, d. h. die möglichen Risiken für die Rechte und Freiheiten der betroffenen Person werden festgelegt. Hierbei werden sowohl die Art, der Umfang, die Umstände sowie der Zweck der Verarbeitung als auch die Eintrittswahrscheinlichkeit einer Gefahr sowie die Auswirkung eines (möglichen) Schadens berücksichtigt.

Jeder Mitarbeiter muss die personenbezogenen Daten in seinem Verantwortungsbereich ausreichend gegen unberechtigten Zugriff bzw. Verarbeitung sowie Verlust schützen (z. B. Passwortsperre, Verschließen von vertraulichen Unterlagen, datenschutzkonforme Vernichtung / Schreddern, aufgeräumter Schreibtisch, Verschlüsselung von E-Mails, sicheres Format beim Versenden (z. B. PDF)).

4 Datenschutz-Prozesse

4.1 Rechte der betroffenen Personen

Die betroffenen Personen, von denen wir personenbezogene Daten verarbeiten (z. B. Kunde, Lieferant, andere Geschäftspartner) haben bezüglich des Datenschutzes die unten dargestellten Rechte. Diese können in Form von Anträgen bei uns geltend gemacht werden. Auskunfts- und Einsichtsrechte von Mitarbeitern werden durch die Personalabteilung erfüllt.

Jeder Mitarbeiter ist verpflichtet, sich mit den entsprechenden Rechten und den internen Prozessabläufen, die in der Anlage detailliert beschrieben sind, vertraut zu machen und danach zu handeln. Sie werden zudem im Rahmen der regelmäßig stattfindenden Mitarbeiterschulungen diesbezüglich sensibilisiert.

Ferner werden die Prozesse regelmäßig in Form von „Feuerwehrübungen“ (Probedurchlauf) geprüft und hinsichtlich Effektivität und Korrektheit kontrolliert, um interne oder Fristprobleme zu beheben.

4.1.1 Recht auf Auskunft

Die betroffene Person hat das Recht gem. Art. 15 DS-GVO eine Bestätigung darüber zu verlangen, ob personenbezogene Daten über sie verarbeitet werden. Wenn dies der Fall ist, so hat sie ein Recht auf Auskunft über diese personenbezogenen Daten.

Zudem müssen wir bei Verlangen eine unentgeltliche Kopie der betreffenden personenbezogenen Daten zur Verfügung stellen. Wenn allerdings Persönlichkeitsrechte anderer Personen entgegenstehen, darf keine Kopie herausgegeben werden.

Wie solche Anträge auf Auskunft bearbeitet werden müssen, ist detailliert in unserem Prozess in der Anlage 1 beschrieben.

4.1.2 Recht auf Berichtigung

Die betroffene Person hat das Recht gem. Art. 16 DS-GVO unverzüglich die Berichtigung der sie betreffenden unrichtigen personenbezogenen Daten zu verlangen (z. B. weil sich die

Adresse geändert hat). Je nach Verarbeitungszweck hat die Person auch das Recht, die Vervollständigung unvollständiger personenbezogener Daten zu verlangen.

Wenn die betroffenen personenbezogenen Daten auch anderen Stellen (z. B. externen Dienstleistern) offengelegt wurden, so müssen auch alle Empfänger über jede Datenberichtigung informiert werden, es sei denn, dass sich dies als unmöglich erweist oder der Aufwand unverhältnismäßig groß ist.

Der Prozess zu Anträgen auf Berichtigung ist in der Anlage 2 beschrieben.

4.1.3 Recht auf Löschung („Recht auf Vergessenwerden“)

Die betroffene Person hat das Recht gem. Art. 17 DS-GVO zu verlangen, dass die über sie gespeicherten Daten unverzüglich gelöscht werden, wenn z. B. die Daten für den Verarbeitungszweck nicht mehr erforderlich sind oder eine Einwilligung widerrufen oder ein Widerspruch eingelegt wurde und keine Aufbewahrungspflichten der Löschung entgegenstehen. Hierüber müssen grundsätzlich auch etwaige Empfänger informiert werden, dies betrifft auch die Löschung von Links zu diesen personenbezogenen Daten oder Kopien bzw. Replikationen.

Ob bzw. wie ein Löschantrag umgesetzt werden muss, ist umfassend in der Prozessbeschreibung in der Anlage 3 beschrieben.

4.1.4 Recht auf Einschränkung der Verarbeitung

Die betroffene Person hat unter bestimmten Voraussetzungen gemäß Art. 18 DS-GVO das Recht, die Einschränkung der Verarbeitung ihrer personenbezogenen Daten zu verlangen. Dies betrifft beispielsweise Fälle, in denen die Richtigkeit der Daten streitig ist, die Verarbeitung der personenbezogenen Daten unrechtmäßig erfolgte oder wenn es um die Geltendmachung, Ausübung oder Verteidigung von rechtlichen Ansprüchen geht.

Wenn die Verarbeitung personenbezogener Daten eingeschränkt wird, dürfen diese personenbezogenen Daten – von ihrer Speicherung abgesehen – nur mit Einwilligung der betroffenen Person oder zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen oder zum Schutz der Rechte anderer natürlicher oder juristischer Personen bzw. aus Gründen eines wichtigen öffentlichen Interesses verarbeitet werden. Hierüber müssen etwaige Empfänger informiert werden.

Wenn eine Einschränkung der Daten erwirkt wurde, so müssen wir als Unternehmen sicherstellen, dass betroffene Personen vor Aufhebung der Einschränkung darüber unterrichtet werden. Wie ein Antrag auf Einschränkung der Verarbeitung bearbeitet werden muss, ist umfassend in dem Prozess in der Anlage 4 beschrieben.

4.1.5 Recht auf Datenübertragbarkeit

Die betroffene Person hat nach Art. 20 DS-GVO das Recht, die sie betreffenden personenbezogenen Daten in einem strukturierten, gängigen und maschinenlesbaren Format zu erhalten.
Das Recht auf Datenübertragbarkeit ist nur dann gegeben, wenn es sich um Daten handelt, die der Betroffene selbst zur Verfügung gestellt hat und die automatisiert auf Basis eines Vertrags oder einer Einwilligung verarbeitet wurden.

Zudem besteht das Recht auf Datenübertragbarkeit nicht, wenn Rechte und Freiheiten anderer Personen betroffen sind.

Anders als bei bestimmten (unbegründeten oder exzessiven) Auskunftsersuchen darf für das Recht auf Datenportabilität kein Entgelt verlangt werden und weil dieser Anspruch gerade nicht an ein Vertragsende gebunden ist, darf es nicht mit einer Kündigung o. Ä. verwechselt werden. Die Geltendmachung dieses Rechts kann zu jedem Zeitpunkt der laufenden Geschäftsbeziehung erfolgen und sollte nicht als Signal gewertet werden, dass der Kunde das Vertragsverhältnis beenden will.

Wie mit Anträgen auf Datenübertragung umgegangen werden muss, ist umfassend in der Prozessbeschreibung in der Anlage 5 beschrieben.

4.1.6 Widerspruchsrecht

Die betroffene Person hat das Recht gem. Art. 21 DS-GVO aus Gründen, die sich aus ihrer besonderen Situation ergeben, gegen die Verarbeitung ihrer personenbezogenen Daten, die aufgrund einer zuvor vorgenommenen Interessenabwägung stattfindet, Widerspruch einzulegen.

Wenn ein diesbezüglicher Widerspruch eingelegt wird, dürfen wir die Daten nicht mehr verarbeiten, es sei denn, dass die Unternehmen wiederum zwingende schutzwürdige Gründe für die Weiterverarbeitung nachweisen können, welche die Interessen, Rechte und Freiheiten der betroffenen Person überwiegen oder wenn die Verarbeitung der Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen dient. Welche Interessen dann letztlich überwiegen, hängt vom Einzelfall ab und muss ggf. im Streitfall behördlich bzw. richterlich geklärt werden.

Bei erfolgtem Widerspruch dürfen die personenbezogenen Daten nicht mehr für den Zweck verarbeitet werden.

Den genauen Ablauf unseres Beschwerdemanagements finden Sie in der Anlage 6.

4.1.7 Recht auf Widerruf von Einwilligungen

Grundsätzlich kann jede erteilte Einwilligung gem. Art. 7, 8 DS-GVO auch widerrufen werden, was zur Folge hat, dass die betreffende Datenverarbeitung nicht mehr stattfinden darf, wenn die Einwilligung die Rechtsgrundlage für die betreffende Datenverarbeitung war. Wichtig ist, dass ein Widerruf unverzüglich umgesetzt wird; dies ist systemseitig entsprechend abzubilden (z. B. im CRM-System, Newsletter-Tool etc.). Zudem muss der Widerruf einer Einwilligung so einfach möglich sein wie die Erteilung der Einwilligung selbst.

Den genauen Ablauf finden Sie in Anlage 7.

4.2 Informationspflichten gegenüber betroffenen Personen

Die DS-GVO schreibt vor, Betroffene umfassend über die Datenverarbeitung des Unternehmens zu informieren. Dies betrifft gerade nicht nur Kunden und Interessenten, sondern gilt auch gegenüber Mitarbeitern, da auch diese im Rechtssinne Betroffene sind, so dass auch Mitarbeiter zu informieren sind.

Wichtig ist, dass bei der Implementierung der Informationspflichten bedacht wird, sämtliche Szenarien und „Kontaktpunkte“ mit allen Gruppen betroffener Personen (s. o. Kunden, Interessenten, Mitarbeiter) zu berücksichtigen, damit sowohl im Online- (z. B. Webseite, Webshop etc.) als auch im Offline-Bereich (stationärer Vertrieb, Messekontakte etc.) und bei telefonischen Kontakten, die Datenerhebungen bei Betroffenen mit sich bringen, Transparenzanforderungen eingehalten werden können.

Was Inhalt, Form und Zeitpunkt der Information angeht, so ergeben sich die Anforderungen an die Betroffeneninformation direkt aus den Artikeln 13 und 14 DS-GVO. Aus diesem Grund sind Texte nach Art. 13, 14 DS-GVO stets individuell zu erstellen.

Den zugehörigen Prozess finden Sie in Anlage 8.

4.3 Automatisierte Entscheidung im Einzelfall einschließlich Profiling

Art. 22 Abs. 1 DS-GVO ordnet an, dass betroffene Personen das Recht haben, nicht einer ausschließlich auf einer automatisierten Verarbeitung beruhenden Entscheidung unterworfen zu werden, die ihr gegenüber rechtliche Wirkung entfaltet oder sie erheblich beeinträchtigt (sogenanntes „Profiling“, z. B. Scoring).

Automatisierte Entscheidungen sind zulässig, wenn dies für den Abschluss oder die Erfüllung eines Vertrags nötig ist oder mit ausdrücklicher Einwilligung der betroffenen Person erfolgt oder aufgrund von Rechtsvorschriften zulässig ist. Bei Einwilligungen ist grundsätzlich Vorsicht geboten, da die DS-GVO diese Rechtsgrundlage anerkennt, jedoch in Art. 7 Abs. 4 DS-GVO betont wird, dass die Einwilligung freiwillig erfolgen muss (sogenanntes „Kopplungsverbot“).

Art. 22 Abs. 3 DS-GVO verlangt, dass wir als Unternehmen angemessene Maßnahmen zum Schutz der Rechte und Freiheiten Betroffener treffen. Dazu zählt mindestens das Recht der Erwirkung des Eingreifens einer Person seitens des Verantwortlichen, das Recht auf Darlegung des eigenen Standpunkts und auf Anfechtung der seitens des Verantwortlichen getroffenen Entscheidung. Dieses sogenannte „Remonstrationsrecht“ bedingt, dass wir als Unternehmen entsprechende Anfragen Betroffener bearbeiten müssen.

Darüber hinaus dürfen laut Art. 22 Abs. 4 DS-GVO Entscheidungen nach Absatz 2 grundsätzlich nicht auf besonderen Kategorien personenbezogener Daten beruhen; eine Ausnahme gilt bei Einwilligungen.

Beachten Sie hierzu den Prozess in Anlage 9.

4.4 Meldepflicht bei Datenpannen

Nach der DS-GVO unterliegen wir bei der Verletzung des Schutzes personenbezogener Daten einer Meldepflicht.

Nach Art. 33 DS-GVO ist entscheidend, ob die Verletzung des Schutzes personenbezogener Daten zu einem Risiko für die Rechte und Freiheiten Betroffener führt.

Die Meldung muss binnen **72 Stunden** an die zuständige Datenschutzaufsichtsbehörde erfolgen, was direkte Auswirkungen für unsere Unternehmensstruktur bzw. Unternehmenskommunikation hat: Daher müssen interne Melde- und Eskalationswege eingehalten werden, um etwaigen Pannen sofort zu begegnen.

Beachten Sie hierzu den Prozess in Anlage 10.

4.5 Outsourcing / Verträge über Auftragsverarbeitung

Bei der Zusammenarbeit mit Dienstleistern, die in unserem Auftrag und auf unsere Weisung hin unsere personenbezogenen (Kunden- / Mitarbeiter- / Online-)Daten verarbeiten, bedarf es einer datenschutzrechtlichen Vereinbarung, eines sogenannten

„Auftragsverarbeitungsvertrags“, der vor Beginn der Zusammenarbeit geschlossen werden muss.

Insgesamt muss jederzeit nachvollziehbar sein, mit welchen Dienstleistern zusammengearbeitet wird und dass ein entsprechendes Vertragswerk samt Dienstleisterprüfungen existiert. Besonderheiten ergeben sich bei Rechtsgrundlagen der Datenübermittlung in sogenannte „Drittstaaten“, die außerhalb der EU bzw. des EWR liegen. Dies betrifft z. B. Dienstleister in den USA. Aufgrund der Komplexität muss das Thema Datentransfers ins Ausland stets gesondert geprüft werden.

Zum genauen Ablauf beachten Sie den Prozess in Anlage 11.

4.6 Verarbeitungsübersicht

Diese im Datenschutz schon lange bekannte Anforderung bekommt wegen der Rechenschaftspflicht der DS-GVO noch mehr Gewicht: Das Verzeichnis von Datenverarbeitungstätigkeiten ist damit ein zentrales Dokument, das zum Nachweis der Rechtskonformität dient.

Art. 30 DS-GVO regelt, welche Informationen enthalten sein müssen. Hierzu stehen entsprechende interne Vorlagen zur Verfügung.

Den zugehörigen Prozess finden Sie in Anlage 12.

4.7 Datenschutz-Folgenabschätzung

Bei risikobehafteten Datenverarbeitungen sieht die DS-GVO vor, dass immer eine Datenschutz-Folgenabschätzung durchzuführen ist.
Daher ist bei der Einführung neuer oder der Änderung bestehender Datenverarbeitungsprozesse eine entsprechende Prüfung durchzuführen.
Eine typische Schwierigkeit in diesem Bereich liegt in der Auslegung des Begriffs des Risikos, zumal aufgrund steigender Datenverknüpfungen diese durch neue technische Möglichkeiten im Bereich Digitalisierung bedingt sind.

Die DS-GVO sieht vor, dass die Aufsichtsbehörden einen Katalog erstellen, der diejenigen Konstellationen benennt, in denen eine Datenschutz-Folgenabschätzung durchzuführen ist – oder auch nicht. Dies bedeutet, dass in bestimmten Fällen, trotz Bestehens eines hohen Risikos für die Rechte und Freiheiten Betroffener, keine Datenschutz-Folgenabschätzung durchzuführen ist.

Die DS-GVO verlangt, dass Maßnahmen, die das Schadens- bzw. Eintrittspotential im Hinblick auf die Rechte und Freiheiten Betroffener reduzieren, zu implementieren sind. Wenn die Bewertung im Rahmen einer Datenschutz-Folgenabschätzung ergibt, dass trotz Schutzmaßnahmen ein Restrisiko verbleibt, ist die Datenschutzaufsicht zu konsultieren. Diese Anforderung ist nicht optional, sondern als Ultima Ratio ein zwingendes Erfordernis.

Beachten Sie hierzu den Prozess in Anlage 13.

4.8 Datenschutzkontrollen

Die Einhaltung der Richtlinien zum Datenschutz und der geltenden Datenschutzgesetze wird regelmäßig durch Datenschutzprüfungen und weitere Kontrollen überprüft.

Die Ergebnisse der Datenschutzkontrollen sind zu dokumentieren.

Die zuständige Datenschutzaufsichtsbehörde kann im Rahmen der ihr nach staatlichem Recht zustehenden Befugnisse auch eigene Kontrollen der Einhaltung der Vorschriften dieser Richtlinie durchführen.

Der Prozess hierzu ist in Anlage 14 beschrieben.

4.9 Definition und ständige Verbesserung der technischen und organisatorischen Maßnahmen

Die DS-GVO verpflichtet Unternehmen, die Datenverarbeitung personenbezogener Daten durch angemessene technische und organisatorische Maßnahmen abzusichern und personenbezogene Daten nach Möglichkeit zu anonymisieren oder zu pseudonymisieren. Die getroffenen Maßnahmen müssen dabei dem Risiko des jeweiligen Datenverarbeitungsvorgangs Rechnung tragen und dem derzeitigen Stand der Technik entsprechen.

Diese Anforderungen können nur durch ein wirksames Zusammenspiel aus Datenschutzmanagement und Informationssicherheitsmanagement erfüllt werden.

Der Prozess hierzu ist in Anlage 15 beschrieben.

4.10 Sicherstellung Privacy by Design / by Default

Neben den Anforderungen im Hinblick auf die Transparenz der Datenverarbeitungsvorgänge, die durch entsprechende Informationspflichten gegenüber Betroffenen erreicht werden soll, ist die datenschutzfreundliche Ausgestaltung von Anwendungen und Systemen – auch bekannt unter dem Begriff „Privacy by Design“ und „Privacy by Default“ – ein weiteres erklärtes Ziel der DS-GVO, das wir als Unternehmen beachten müssen:

„Privacy by Design“ meint Datenschutz durch Technikgestaltung. Bei der konkreten Produkt- und / oder Anwendungsgestaltung kann dies nur durch eine frühzeitige, durchgängige und konsequente Berücksichtigung datenschutzrechtlicher Anforderungen erreicht werden. Mit anderen Worten müssen Datenschutz- und Datensicherheitsthemen von Anfang an bedacht werden, was sich sowohl im Budget als auch in den Ressourcen widerspiegeln muss.

„Privacy by Default“ bezieht sich auf datenschutzfreundliche Grundeinstellungen. Diese kann durch die Umsetzung von „Privacy by Design“ erreicht werden, wodurch verdeutlicht wird, dass diese beiden Aspekte voneinander abhängig sind. Nutzer unserer Anwendungen und Produkte sollen jederzeit darauf vertrauen können, dass Datenschutz- und Datensicherheitsanforderungen gewahrt sind und zwar auch ohne dass vorgegebene Werkseinstellungen geändert werden müssen, sondern „per Default“ gegeben sind.

Beachten Sie hierzu den Prozess in Anlage 16.

4.11 Mitarbeitersensibilisierung

Jeder Mitarbeiter, der Umgang mit personenbezogenen Daten hat, ist auf einen vertraulichen Umgang mit personenbezogenen Daten und die Einhaltung dieser Richtlinie zu verpflichten.
Mitarbeiter, die besonderen Geheimhaltungsverpflichtungen (z. B. Fernmeldegeheimnis) unterliegen, werden von den Vorgesetzten ergänzend schriftlich verpflichtet.
Die Einhaltung regulatorischer Anforderungen kann allgemein nur durch eine ausreichende Sensibilisierung der Mitarbeiter erreicht werden, die durch Unterweisungen und Schulungen erfolgt.

In unseren Unternehmen werden die Sensibilisierungsmaßnahmen in regelmäßigen Zeitabständen angeboten, in der Regel jährlich. Bei Neueinstellung oder Stellenwechsel innerhalb des Unternehmens erfolgt stets eine Unterweisung.

Der Prozess hierzu ist in Anlage 17 festgeschrieben.

5 Schlussbestimmungen

Die Anlage zu dieser Datenschutz-Richtlinie besteht aus detaillierten Prozessbeschreibungen zu verschiedenen Datenschutzthemen. Sie werden regelmäßig überprüft und gegebenenfalls aktualisiert. Sie haben den gleichen Geltungsbereich wie diese Richtlinie und sind jeweils ab dem Zeitpunkt ihrer Veröffentlichung gültig.

Die Einhaltung der in dieser Richtlinie enthaltenen Regelungen gehört zu Ihren Arbeitspflichten. Verstöße können mit arbeitsrechtlichen Konsequenzen geahndet werden.

Druck+Verlag Ernst Vögel GmbH /
Binderei und Versand Ernst Vögel GmbH /
Vögel GmbH & Co. KG /
VOB-Verlag Vögel OHG

Stamsried, Oktober 2024

_____	_____
Frau Barbara Bucher (Geschäftsführerin)	Frau Karin Bucher (Geschäftsführerin)

Anlage 1: Prozess Recht auf Auskunft

Prozessbeschreibung:

1. Antrag der betroffenen Person

Die betroffene Person kann sich mit ihrem Antrag auf Auskunft an die Unternehmen wenden. Hierbei kommen die unterschiedlichen Kommunikationskanäle (z. B. Post, E-Mail, Telefon) in Betracht. Es kann sein, dass hierbei die zentralen Kontaktdaten (Firmenimpressum) verwendet werden, es ist aber auch denkbar, dass sich ein bereits bestehender Geschäftskontakt an seinen Ansprechpartner in der jeweiligen Fachabteilung wendet.

Den Antrag auf Auskunft erkennen Sie daran, dass die Person entweder eine Bestätigung verlangt, ob überhaupt personenbezogene Daten über sie verarbeitet werden oder aber ganz gezielt Auskunft über die sie betreffenden personenbezogenen Daten fordert.

Sollten große Datenmengen von personenbezogenen Daten über die betroffene Person gespeichert werden, so kann von dieser verlangt werden, dass sie präzisiert, auf welche Informationen oder Verarbeitungsvorgänge sich ihr Auskunftsersuchen bezieht.

2. Weiterleitung an die zuständige Stelle

Der Antrag auf Auskunft muss unverzüglich an Frau Barbara Bucher weitergeleitet werden. Dies geschieht per E-Mail. Sollte ein Telefonat mit dem Betroffenen stattgefunden haben, ist der Inhalt dieses Gesprächs in einer E-Mail zusammenzufassen und an Frau Barbara Bucher zu senden.

Wichtig ist, dass der Antrag nachweislich und erkennbar weitergeleitet wird, daher muss eine E-Mail im Betreff besonders gekennzeichnet werden.
Für die Fristwahrung und Dokumentation ist es wichtig, in der E-Mail auch die Eingangszeit des Antrags sowie die Art des Eingangs zu vermerken.

3. Identitätsprüfung/Prüfprozess

Zunächst muss die Identität der betroffenen Person von der zuständigen Stelle, Frau Barbara Bucher, in geeigneter Weise überprüft werden. Dies geschieht im Regelfall durch Abfrage der Kundennummer und Vergleich dieser mit den vorhandenen Informationen über die betroffene Person. Welche Methode der Überprüfung geeignet ist, ist je nach Einzelfall zu beurteilen.

Kann die betroffene Person nicht identifiziert werden, ist diese von Frau Barbara Bucher darüber zu unterrichten, damit sie ggf. zusätzliche Informationen bereitstellen kann, die eine Identifikation ermöglichen. Aus Nachweiszwecken sollte die Unterrichtung per Post oder E-Mail erfolgen. Wichtig ist, dass auch die Gründe dokumentiert werden, warum die Person nicht identifiziert werden konnte.

Wenn trotz entsprechender Unterrichtung keine Identifikation möglich ist, besteht kein weiterer Handlungsbedarf mehr.

4. Einbindung des Datenschutzbeauftragten

Bei klärungsbedürftigen Auskunftsverlangen ist vor Auskunftserteilung Rücksprache mit dem Datenschutzbeauftragten zu halten.

5. Ergreifen von Maßnahmen / Beteiligung weiterer Abteilungen / Inhalt des qualifizierten Auskunftsverlangens

Die zuständige Stelle prüft den Auskunftsanspruch. Der Inhalt des Auskunftsschreibens ergibt sich aus dem Gesetz und ist in untenstehender Tabelle mit entsprechendem Prüfschema zusammengefasst. Gegebenenfalls muss eine weitere Abteilung eingebunden werden, damit über alle erforderlichen Punkte Auskunft gegeben werden kann. Wenn dies der Fall ist, gilt auch hier, dass aus Nachweisgründen die Kommunikation per E-Mail erfolgt.

Prüfung	**Auskunft enthält folgende Informationen**
Welche Daten gibt es?	Datenkategorien
Warum werden sie verarbeitet?	Verarbeitungszwecke
Wer erhält die Daten?	Empfänger / Empfängerkategorien
Gehen die Daten an ein Drittland oder eine internationale Organisation?	Garantien für Drittland
Wie lange werden die Daten gespeichert?	Konkrete Dauer oder Kriterium für Dauer
Gibt es Betroffenenrechte?	Bestehen eines Rechts auf: Berichtigung Löschung Einschränkung der Verarbeitung Widerspruchsrecht Beschwerderecht bei Aufsichtsbehörde
Wo kommen die Daten her?	Vom Betroffenen direkt oder von anderen Stellen? Wenn Letzteres der Fall ist => alle verfügbaren Informationen über die Herkunft der Daten
Gibt es automatisierte Entscheidung im Einzelfall (Profiling)?	Logik, Tragweite, Auswirkung für Betroffenen

Es ergeben sich nun zwei Handlungsmöglichkeiten:

1. Die Unternehmen werden nicht tätig, weil keine personenbezogenen Daten über die Person gespeichert sind und teilen dies der betroffenen Person unter Angabe der Gründe mit; es ist ferner auf die Möglichkeit des Beschwerderechts bei der Aufsichtsbehörde sowie Einlegung eines Rechtsbehelfs zu informieren.

2. Die Unternehmen werden tätig: Das qualifizierte Auskunftsverlangen muss erteilt werden, da personenbezogene Daten über die betroffene Person vorliegen.

6. Rückmeldeprozess an die betroffene Person / Frist / Form

- **Es sind keine personenbezogenen Daten vorhanden:**

Wenn keine personenbezogenen Daten über die Person gespeichert werden, wird dies durch Frau Barbara Bucher der betroffenen Person unter Angabe der Gründe unverzüglich, spätestens innerhalb eines Monats nach Eingang des Antrags mitgeteilt (sog. „Negativauskunft").

- **Es sind personenbezogene Daten vorhanden**:

Wenn personenbezogene Daten vorliegen, werden die gesetzlich erforderlichen Informationen (qualifizierter Auskunftsanspruch) der betroffenen Person unverzüglich, spätestens innerhalb eines Monats nach Eingang des Antrags durch Frau Barbara Bucher mitgeteilt.

Ausnahmsweise kann die Rückmeldung innerhalb von zwei weiteren Monaten erfolgen, wenn die Anzahl der Anträge und deren Komplexität es erforderlich macht. In diesem Fall muss die betroffene Person aber innerhalb eines Monats nach ihrem Antrag darüber informiert werden, dass die Bearbeitung länger dauern wird; die Gründe für die Verzögerung sind ebenfalls zu nennen. Insgesamt sind so im Ausnahmefall drei Monate zur Rückmeldung gegeben.

Form:

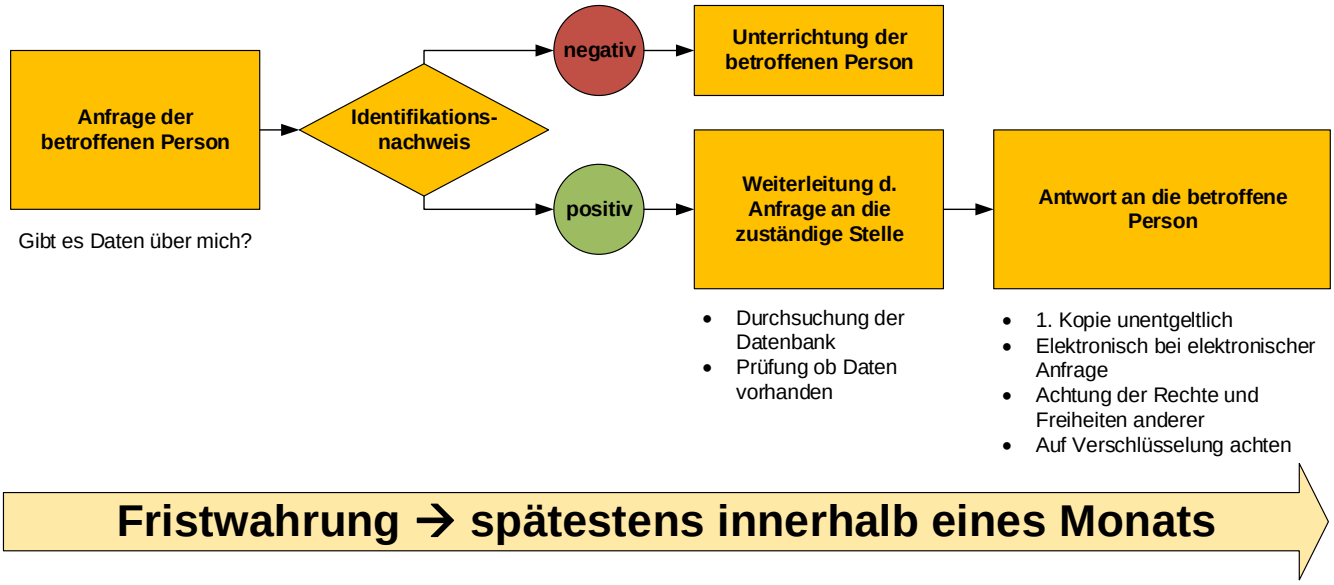
Stellt die betroffene Person den Antrag auf Auskunft elektronisch (z. B. E-Mail), so ist auch die Rückmeldung in einem gängigen elektronischen Format zur Verfügung zu stellen, sofern nichts Abweichendes von der betroffenen Person gewünscht ist.

Die Rückmeldung per E-Mail muss verschlüsselt erfolgen (z. B. verschlüsselter Anhang, separate Mitteilung des Passworts). Bei Fragen hierzu hilft der Datenschutzbeauftragte weiter.

Die Auskunft muss grundsätzlich unentgeltlich erfolgen. Außerdem muss eine Kopie der betreffenden personenbezogenen Daten unentgeltlich zur Verfügung gestellt werden.
Für weitere beantragte Kopien kann ein angemessenes Entgelt für die Verwaltungskosten verlangt werden.
Wenn allerdings Persönlichkeitsrechte anderer Personen entgegenstehen, darf keine Kopie herausgegeben werden.

Auch für die Auskunftserteilung kann in besonderen Fällen ein Entgelt für die Verwaltungskosten für die Unterrichtung, Mitteilung oder Durchführung der Maßnahme verlangt werden. Dies gilt aber nur für offenkundig unbegründete oder exzessive Anträge (im Falle häufiger Wiederholung). Alternativ kann in diesen Fällen auch der Antrag verweigert werden. Die Unternehmen haben den Nachweis für den offenkundig unbegründeten oder exzessiven Charakter des Antrags zu erbringen. In diesen Sonderfällen ist jedoch stets mit dem Datenschutzbeauftragten Rücksprache zu halten. Denn wenn der Antrag doch begründet war und nicht fristgerecht erteilt wurde, kann ein Bußgeld verhängt werden.

Schaubild:



Fristwahrung → spätestens innerhalb eines Monats

zurück

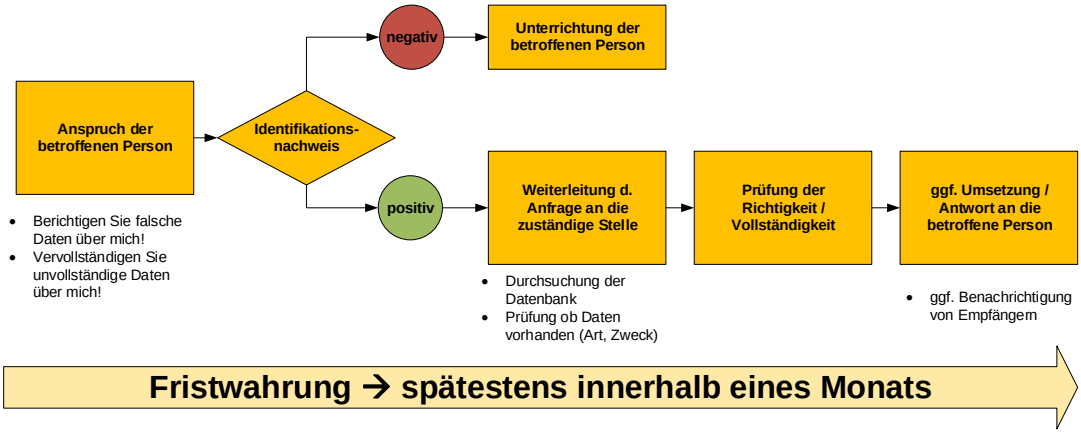
Anlage 2: Prozess Recht auf Berichtigung

Prozessbeschreibung:

Den Antrag auf Berichtigung der Daten erkennen Sie daran, dass die Person die unverzügliche Berichtigung oder Vervollständigung ihrer Daten verlangt (z.B. weil sich ihre Adresse / Telefonnummer etc. geändert hat). Diese Fälle sind von dem jeweiligen Mitarbeiter selbst zu bearbeiten und eine Korrektur kann hier ohne Weiterleitung an Frau Barbara Bucher erfolgen.

Bei schwierigen oder unklaren Sachverhalten kann jedoch selbstverständlich Frau Barbara Bucher zu Rate gezogen werden.

Schaubild:



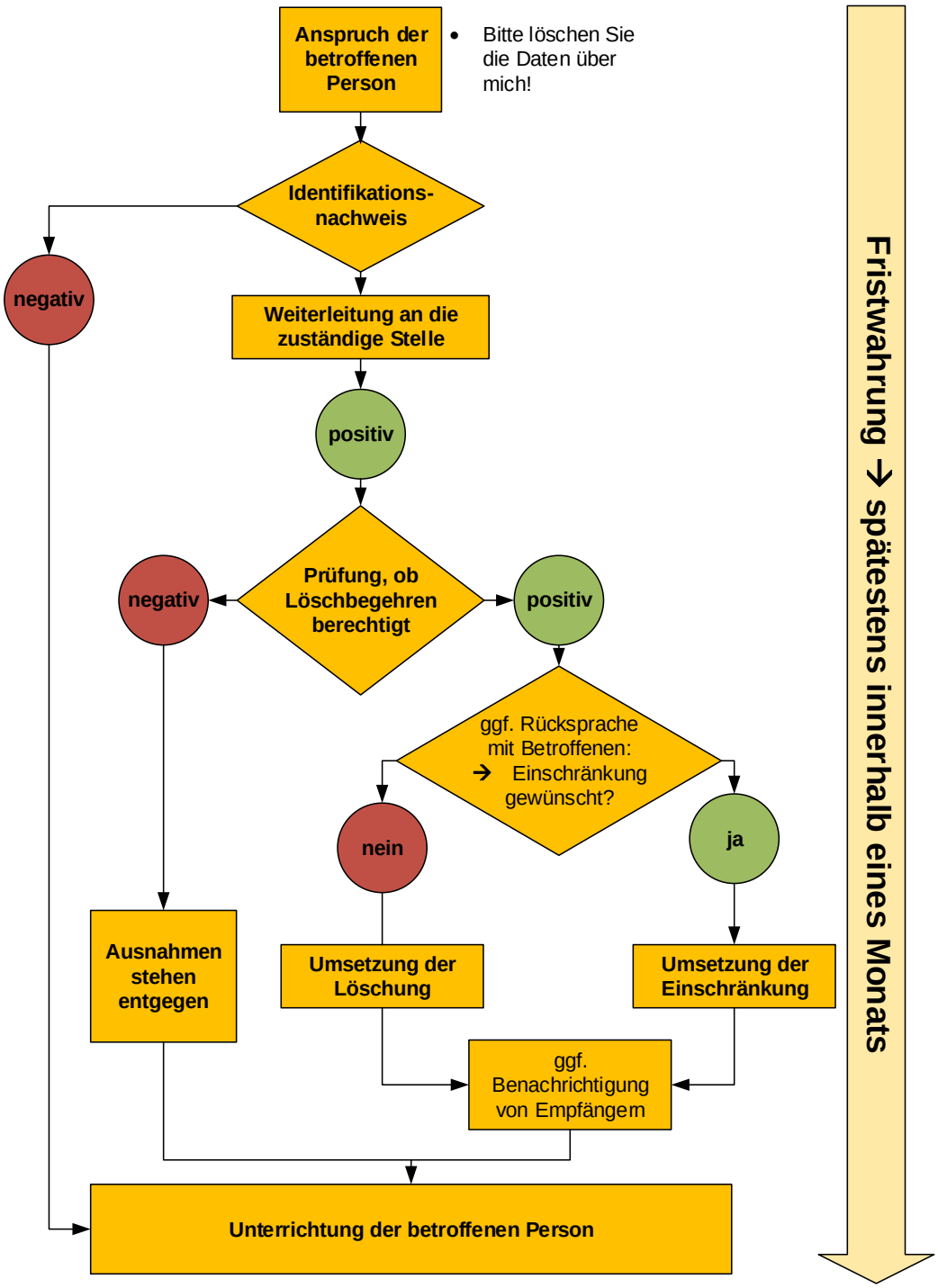
zurück

Anlage 3: Prozess Recht auf Löschung

Prozessbeschreibung:

Den Antrag auf Löschung personenbezogener Daten erkennen Sie daran, dass die Person fordert, dass ihre Daten gelöscht werden.
Zum Ablauf siehe Anlage 1 „Prozess Recht auf Auskunft“.

Schaubild:



zurück

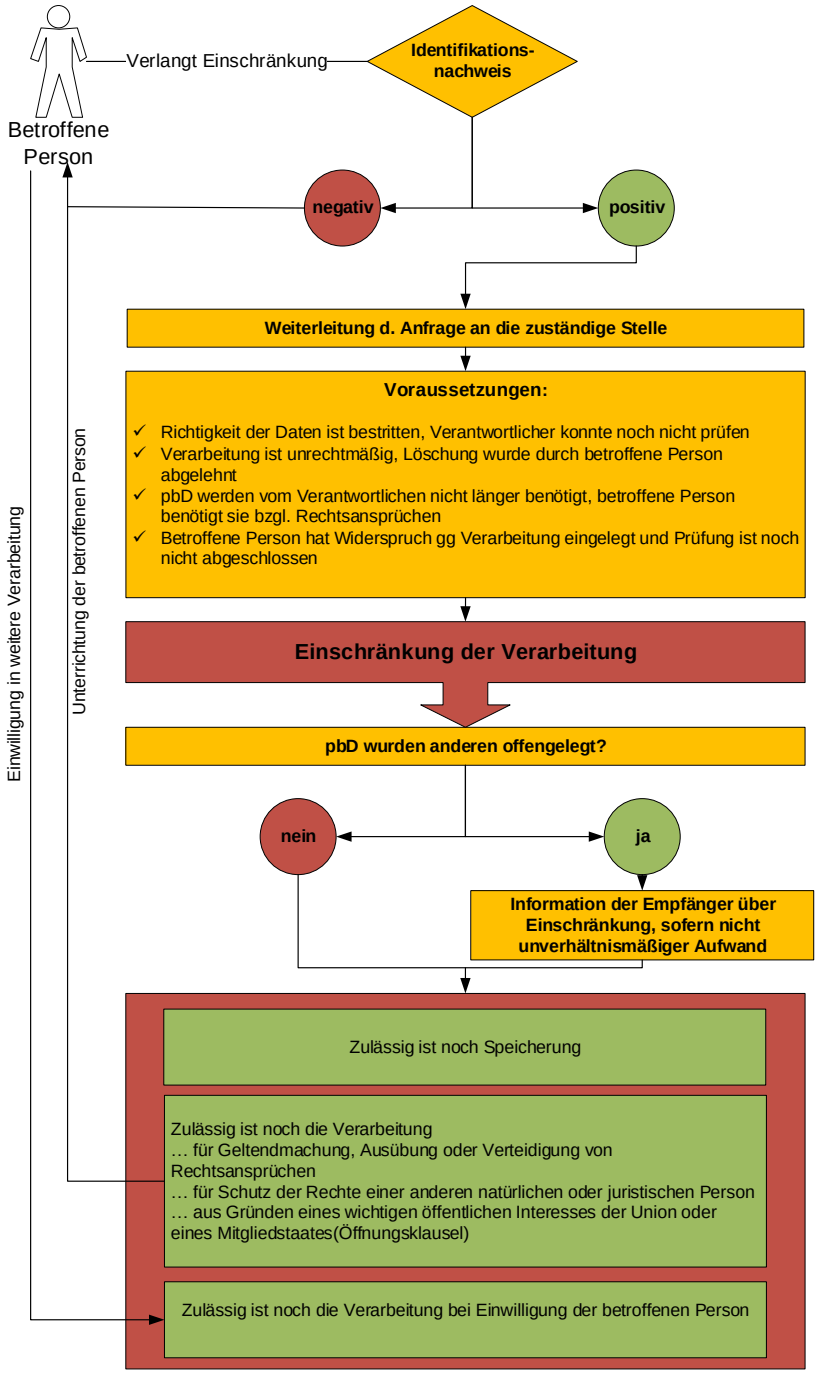
Anlage 4: Prozess Recht auf Einschränkung der Verarbeitung

Prozessbeschreibung:

Den Antrag auf Einschränkung der Datenverarbeitung erkennen Sie daran, dass die Person fordert, dass ihre Daten für einen Teilbereich, d.h. für einen bestimmten Verarbeitungszweck, nicht mehr genutzt werden dürfen, z. B. für Werbezwecke.

Zum Ablauf siehe Anlage 1 „Prozess Recht auf Auskunft“.

Schaubild:



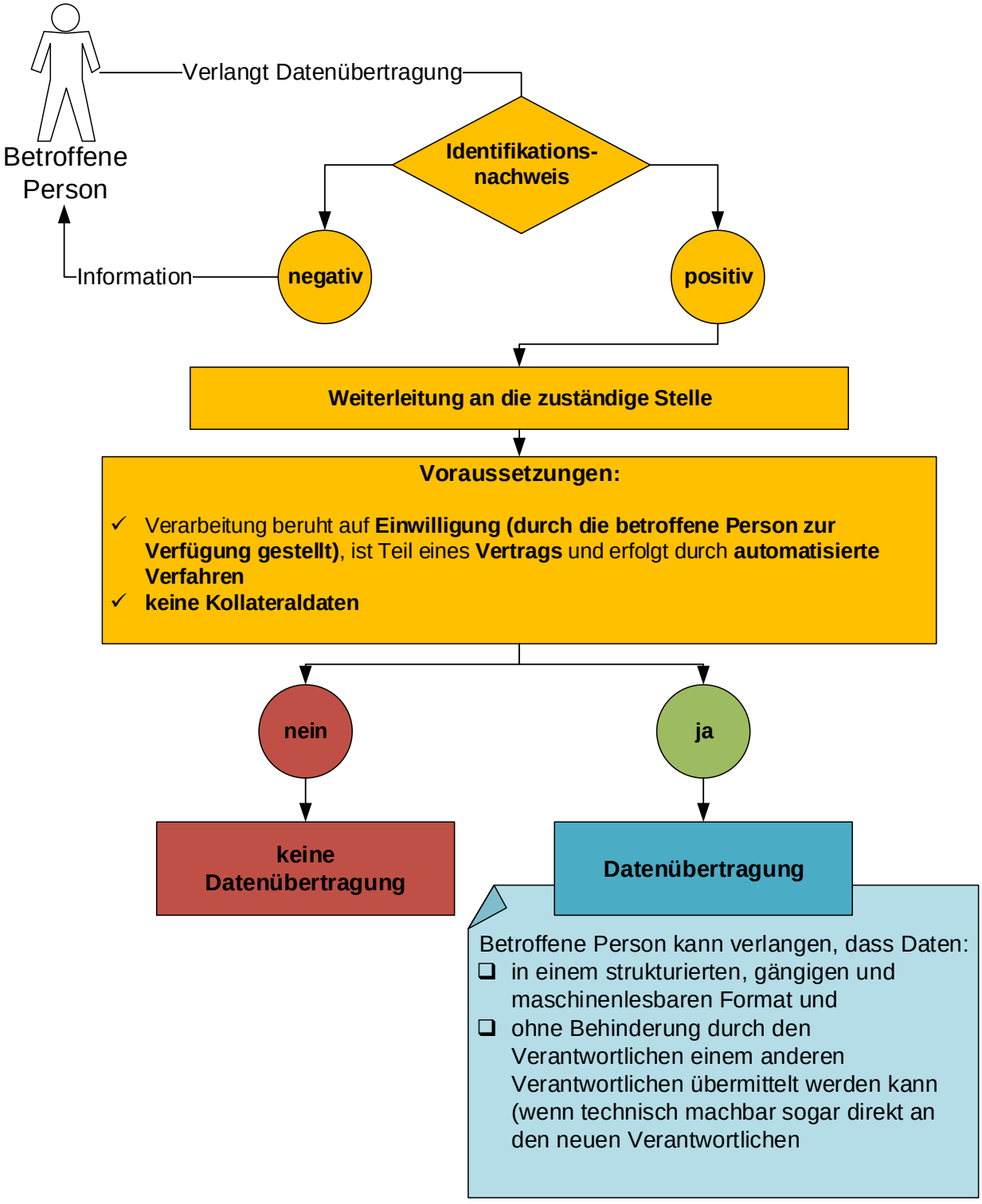
zurück

Anlage 5: Prozess Recht auf Datenübertragbarkeit

Prozessbeschreibung:

Keine weitere Prozessbeschreibung notwendig.

Schaubild:



zurück

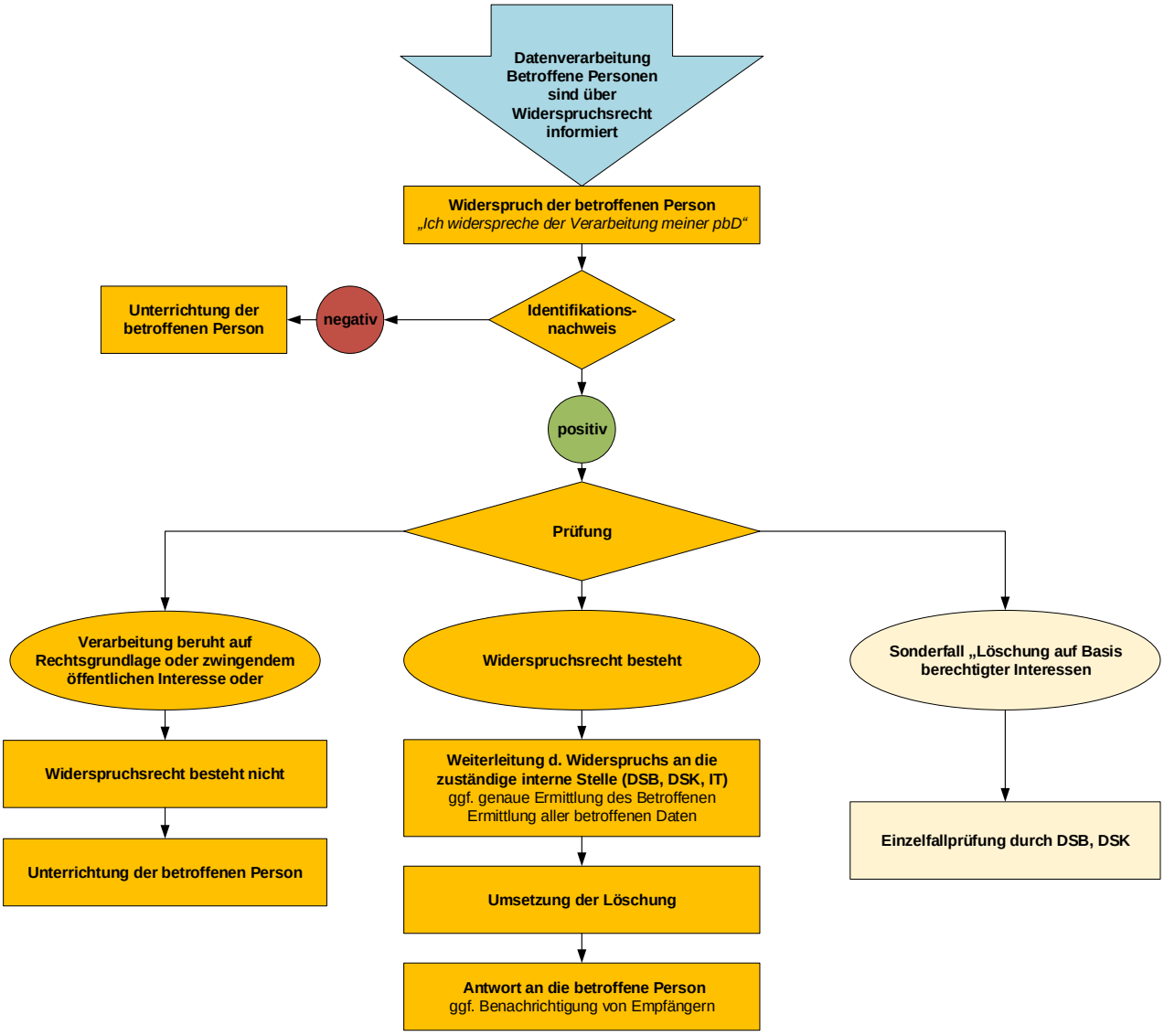
Anlage 6: Prozess Recht auf Widerspruch

Prozessbeschreibung:

Den Widerspruch erkennen Sie daran, dass die Person fordert, dass ihre Daten nicht mehr für die angegebenen Zwecke verarbeitet werden dürfen.

Zum Ablauf siehe Anlage 1 „Prozess Recht auf Auskunft“.

Schaubild:



zurück

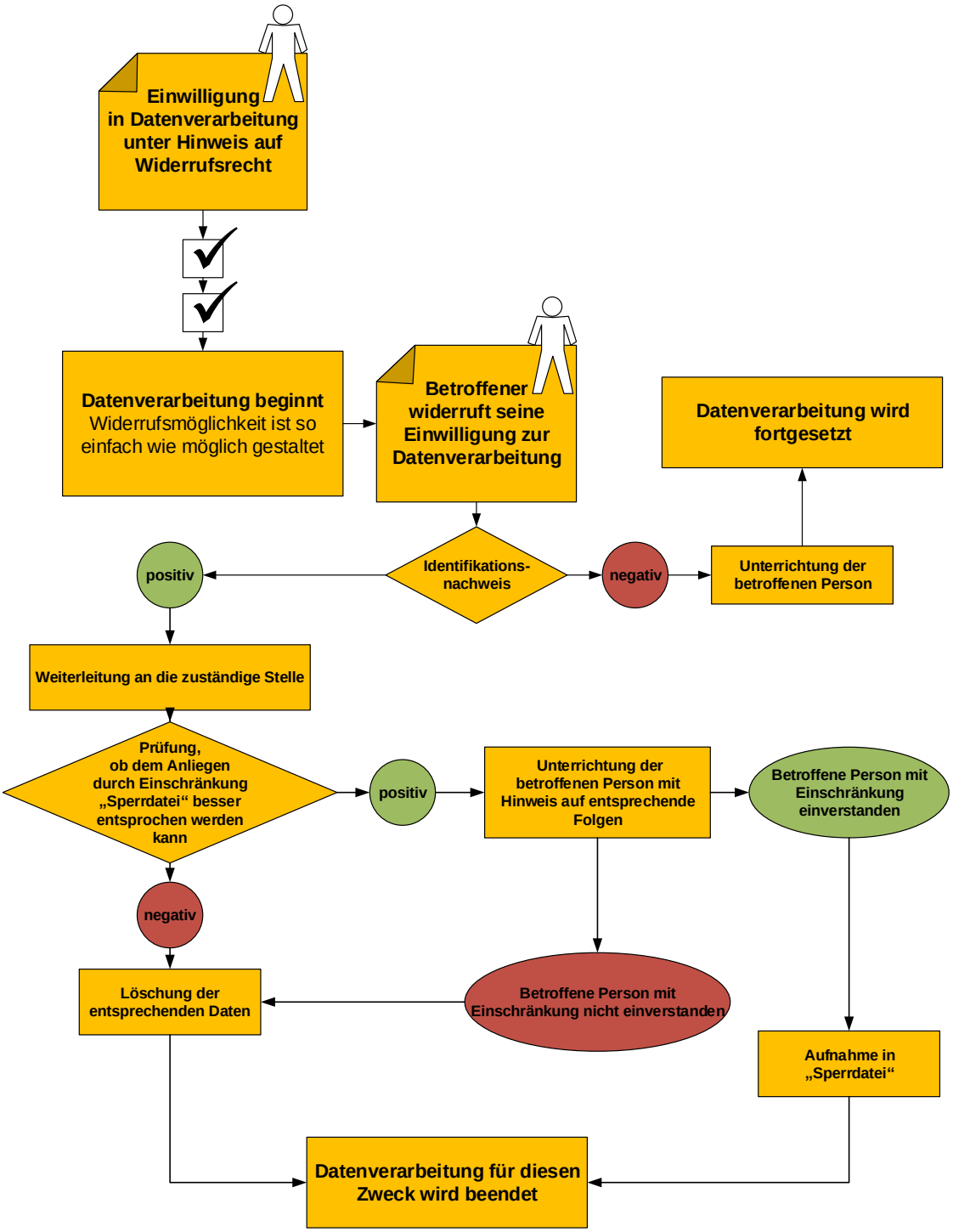
Anlage 7: Prozess Recht auf Widerruf

Prozessbeschreibung:

Den Widerruf erkennen Sie daran, dass die Person fordert, dass ihre Daten nicht mehr für die mit der Einwilligung angegebenen Zwecke genutzt werden dürfen.

Zum Ablauf siehe Anlage 1 „Prozess Recht auf Auskunft“.

Schaubild:



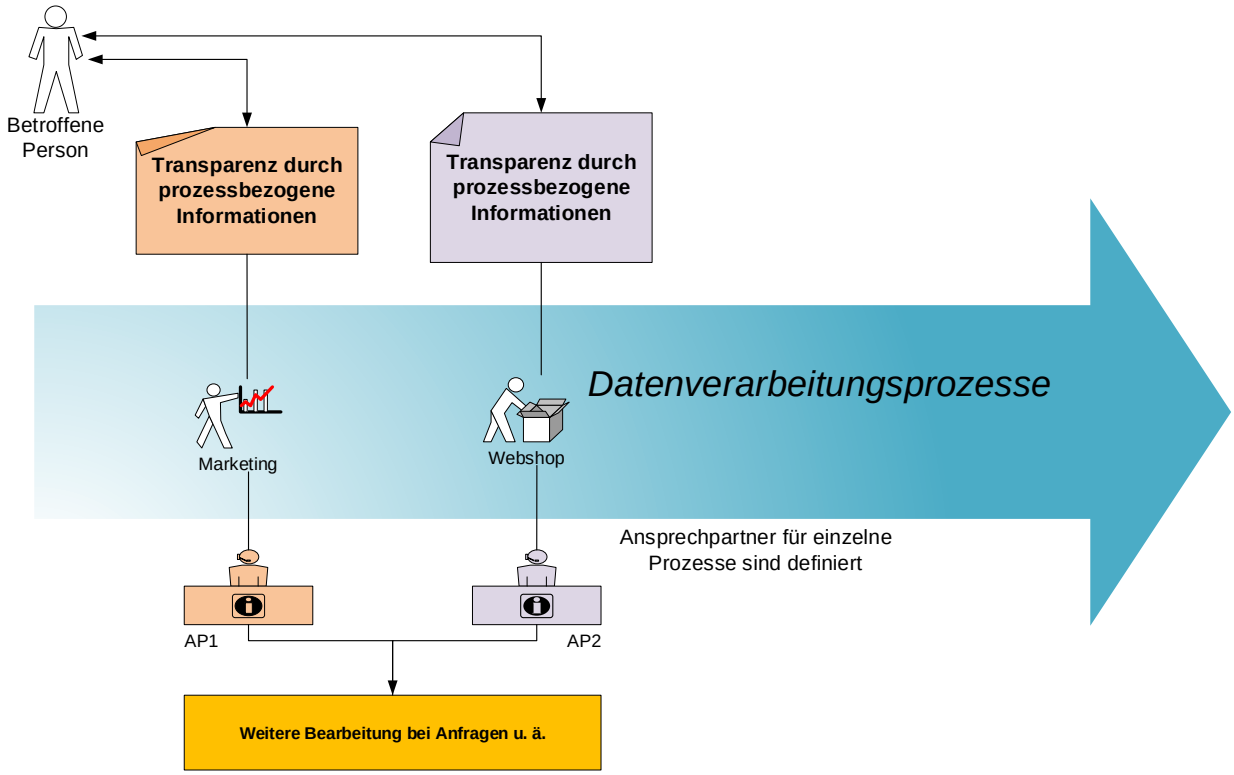
zurück

Anlage 8: Prozess Informationspflichten gegenüber betroffenen Personen

Prozessbeschreibung:

Es wurden Informationen für Bewerber, Praktikanten, Mitarbeiter und Kunden/Vertragspartner/Interessenten erstellt.
Die Hinweise für Bewerber werden diesen nach Eingang der Bewerbung zugesandt.
Die Informationen für Mitarbeiter und Praktikanten werden diesen jeweils zu Beginn des Beschäftigungsverhältnisses bzw. des Praktikums ausgehändigt.
Die Kunden/Vertragspartner/Interessenten erhalten die Informationen als Anhang zu ihrem jeweiligen Angebot per E-Mail.
Alle Informationen befinden sich darüber hinaus auf dem Laufwerk I, auf das alle Mitarbeiter Zugriff haben.

Schaubild:



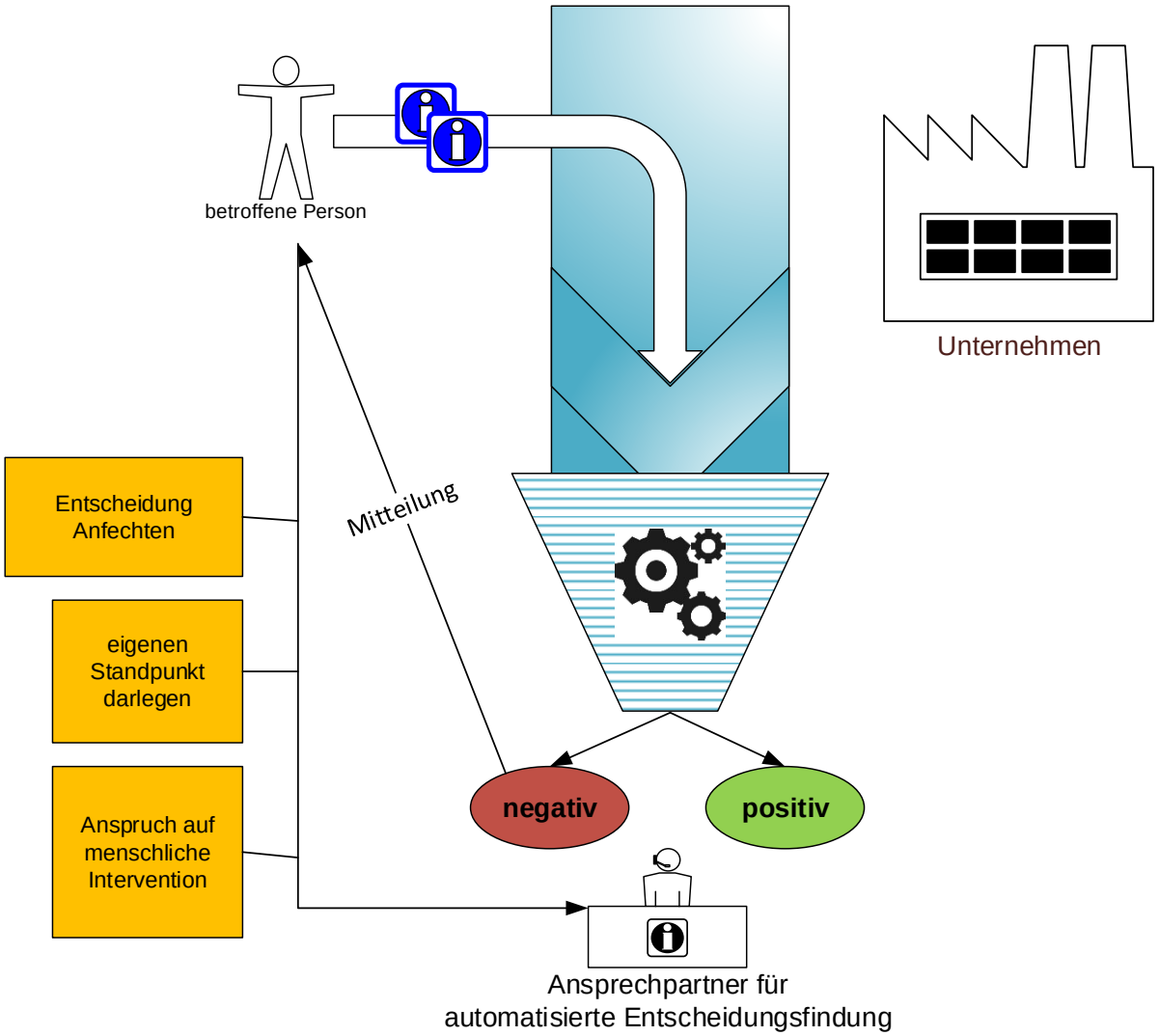
zurück

Anlage 9: Prozess Automatisierte Entscheidung im Einzelfall einschließlich Profiling

Prozessbeschreibung:

Eine automatisierte Einzelfallentscheidung findet nicht statt.

Schaubild:



zurück

Anlage 10: Prozess Meldepflicht bei Datenpannen

Prozessbeschreibung:

1. Kenntniserlangung von Datenpannen

Sobald Sie den Verdacht haben, dass eine Datenpanne vorliegen könnte, haben Sie Ihren Vorgesetzten / Frau Barbara Bucher zu informieren!
Als Datenpanne kommen u. a. in Betracht:

- **Verlust Laptop, Smartphone,**
- **Verschicken von E-Mail mit vertraulichen personenbezogenen Daten an falschen Empfänger,**
- **Abhandenkommen (Verlust, Hacking etc.) von Daten, usw.**

2. Bewertung

Sobald in den Unternehmen die mögliche Verletzung des Schutzes personenbezogener Daten betroffener Personen (Datenpanne) erkannt wird, muss geprüft werden, ob dies voraussichtlich zu einem Risiko für die Rechte und Freiheiten der natürlichen Personen führt. Für die rechtliche Bewertung, ob ein Risiko vorliegt, muss der Datenschutzbeauftragte zu Rate gezogen werden.

3. Maßnahmen zur Abwendung/Eindämmung

Es müssen alle technischen und organisatorischen Maßnahmen ergriffen werden, um das Risiko für die betroffenen Personen einzudämmen.

4. Entscheidung, ob eine Meldung erfolgen soll

Die Entscheidung, ob eine Meldung erfolgen soll, treffen der Datenschutzbeauftragte und die Unternehmensleitung.

5. Meldung an die Aufsichtsbehörde oder den Betroffenen

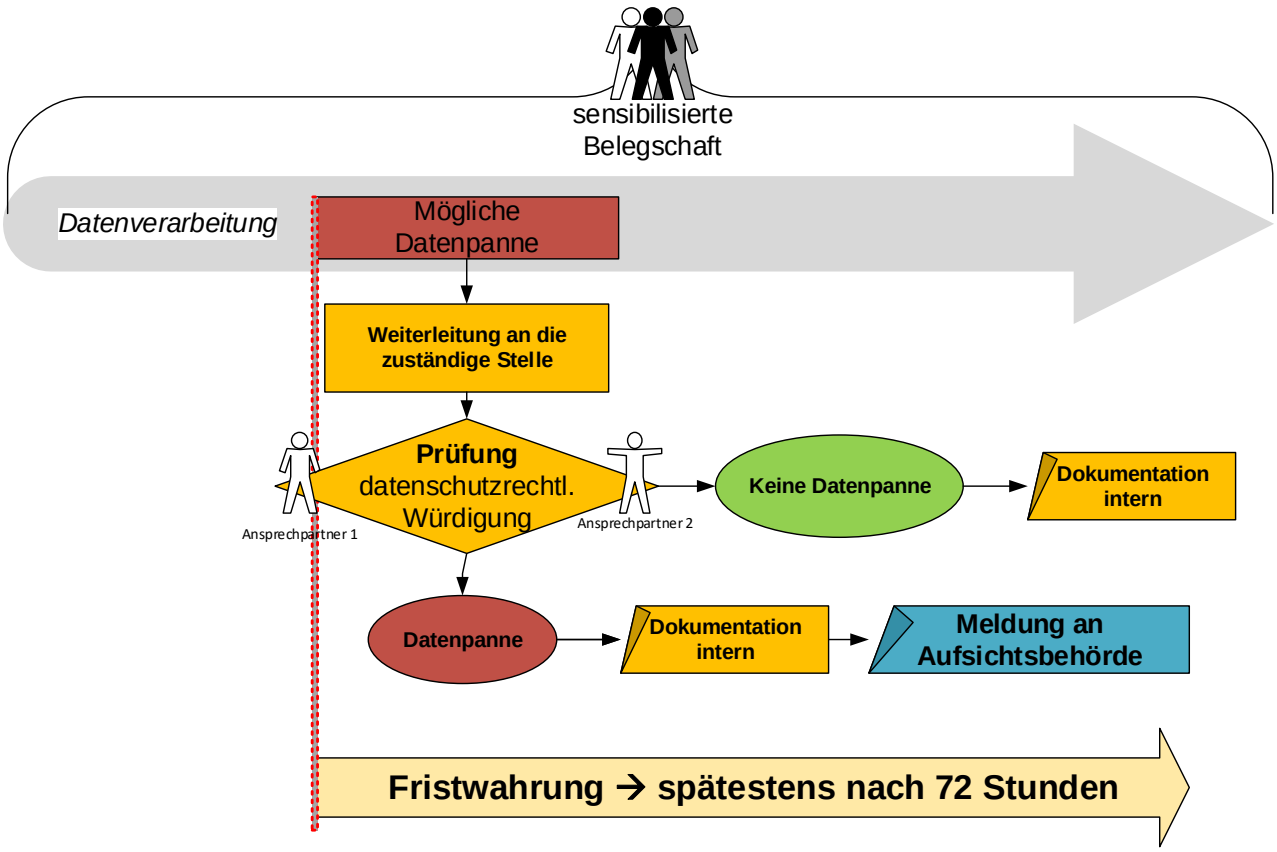
Sofern ein solches Risiko vorliegt, muss innerhalb von 72 Stunden die zuständige Datenschutzaufsichtsbehörde über die Datenpanne informiert werden.
Bei einem hohen Risiko für die Rechte und Freiheiten des Betroffenen, muss dieser zusätzlich direkt und unverzüglich informiert werden. Die Meldung an den Betroffenen entfällt nur wenn,

- vorher geeignete technische und organisatorische Sicherheitsvorkehrungen für die betroffenen Daten vorlagen, vor allem gegen den Zugriff unberechtigter Dritter (z.B. Verschlüsselung)
- oder im Nachgang sichergestellt wird, dass das hohe Risiko für Rechte und Freiheiten der Betroffenen nicht mehr besteht
- oder die Benachrichtigung des Betroffenen mit unverhältnismäßigem Aufwand verbunden wäre.

6. Dokumentation

Zusätzlich wird die Datenpanne, unabhängig davon, ob eine Meldung erfolgt oder nicht, einschließlich aller damit zusammenhängenden Fakten, Folgen und Gegenmaßnahmen vom Unternehmen so dokumentiert, dass die Aufsichtsbehörde die Einhaltung des Artikels überprüfen kann.

Schaubild:



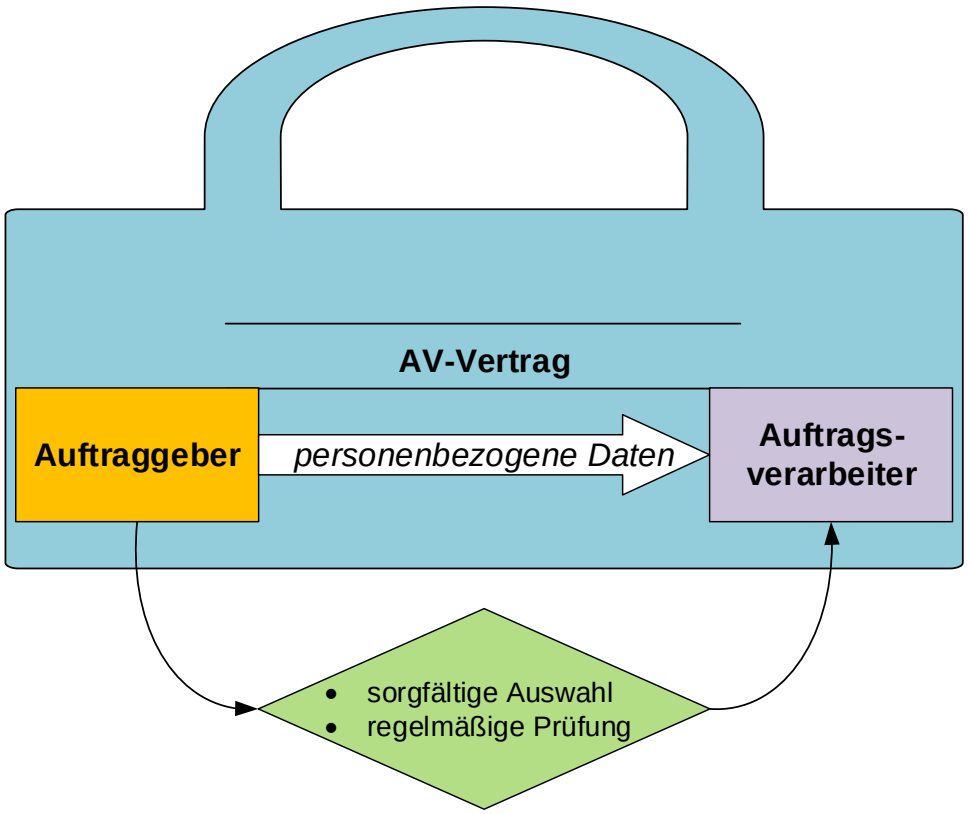
zurück

Anlage 11: Prozess Outsourcing / Verträge über Auftragsverarbeitung

Prozessbeschreibung:

Mit externen Dienstleistern werden Verträge über Auftragsverarbeitung gemäß Art. 28 DS-GVO abgeschlossen. Zuständig hierfür ist die Unternehmensleitung.

Schaubild:



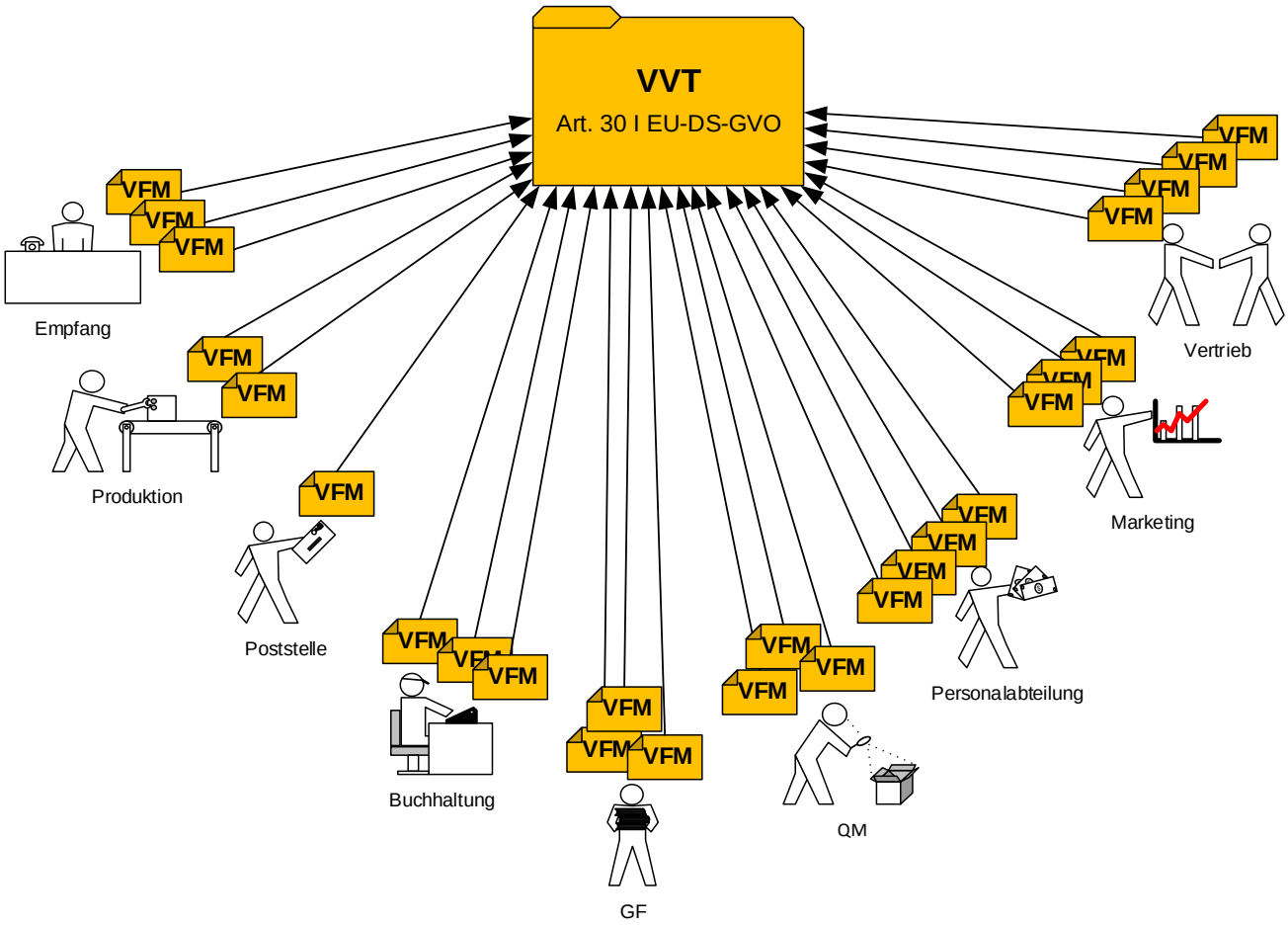
zurück

Anlage 12: Prozess Verarbeitungsübersicht

Prozessbeschreibung:

Das Verzeichnis von Verarbeitungstätigkeiten wurde gemeinsam mit dem Datenschutzbeauftragten erstellt. Dieses stellt eine Dokumentation über sämtliche Verarbeitungsvorgänge innerhalb der Unternehmen dar. Das Verzeichnis wird regelmäßig auf Aktualität geprüft und überarbeitet.

Schaubild:



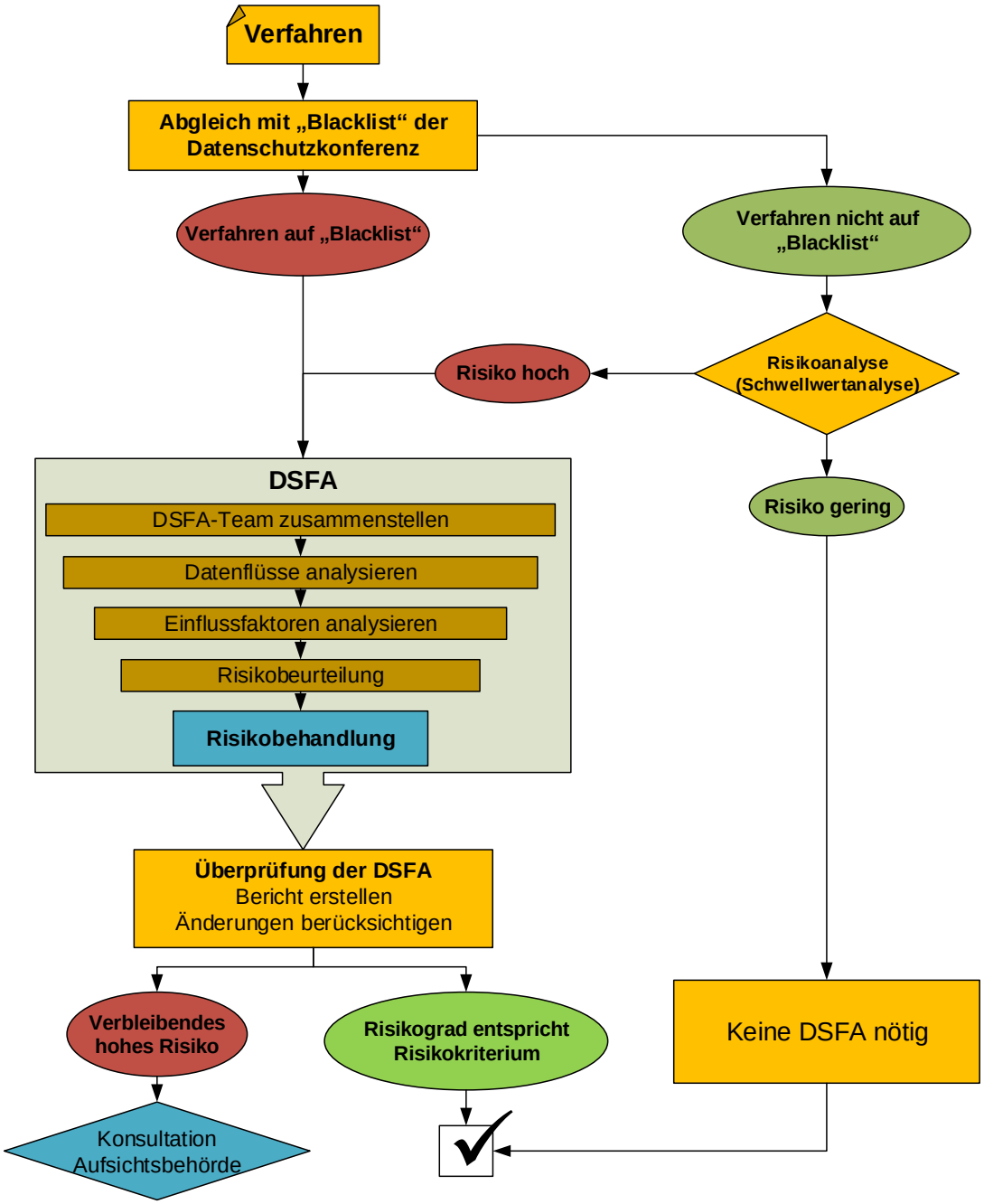
zurück

Anlage 13: Prozess Datenschutz-Folgenabschätzung (DSFA)

Prozessbeschreibung:

Eine Datenschutz-Folgenabschätzung ist bei Verfahren durchzuführen, die voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge haben. Sollte eine solche Prüfung und Risikoeinschätzung notwendig sein, erfolgt eine solche in Zusammenarbeit mit dem Datenschutzbeauftragten.

Schaubild:



zurück

Anlage 14: Prozess Datenschutzprüfungen

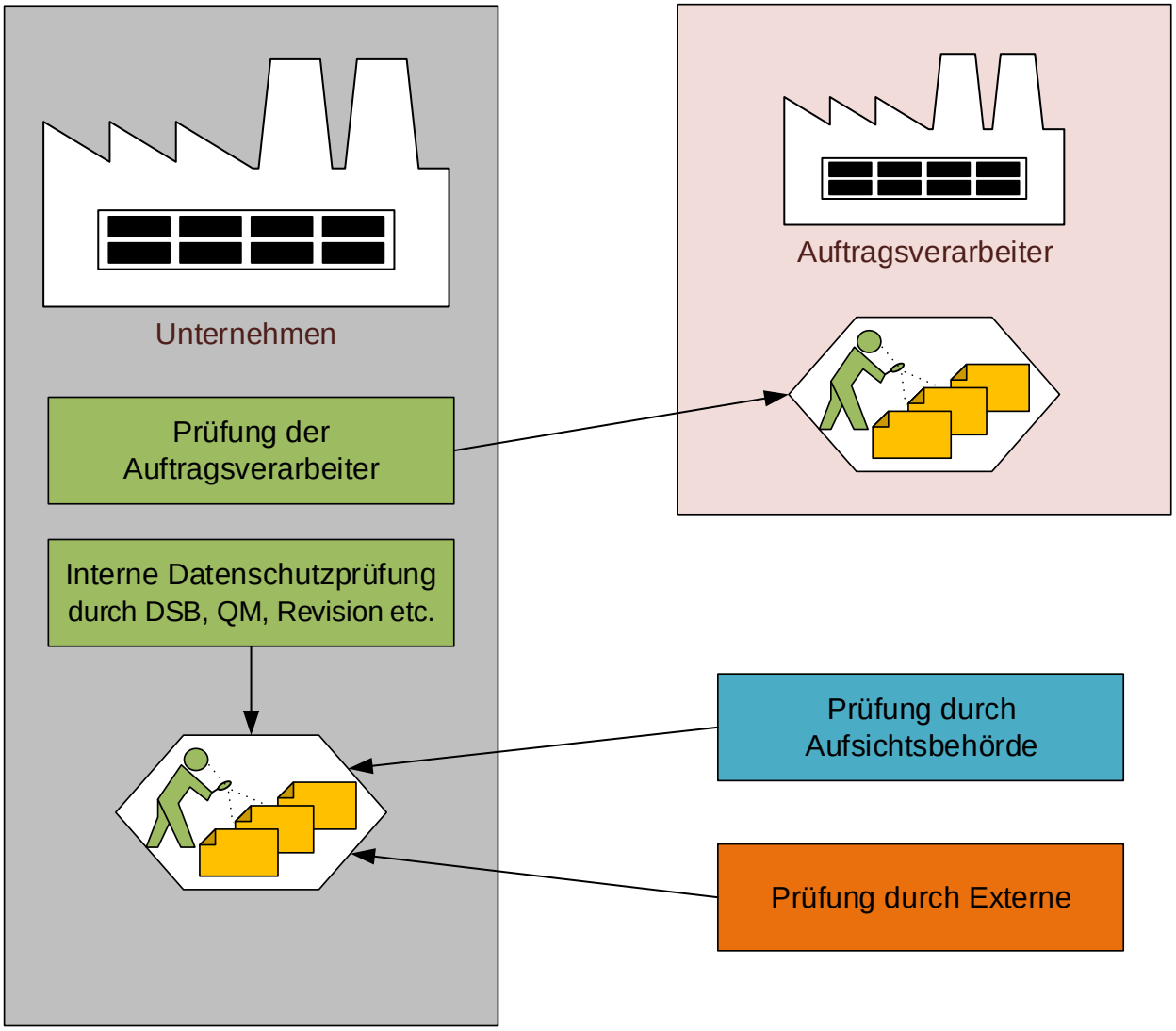
Prozessbeschreibung:

1. Interne Datenschutzprüfungen
Der Datenschutzbeauftragte wird in regelmäßigen Abständen die internen Prozesse in den Unternehmen überprüfen. Diese sogenannten „Feuerwehrübungen“ sollen dazu beitragen, eventuelle Schwachstellen innerhalb der Unternehmen zu identifizieren.

2. Prüfung der Auftragsverarbeiter
Der Datenschutzbeauftragte unterstützt bei der Prüfung der Auftragsverarbeiter, die von den Unternehmen eingesetzt sind.

3. Prüfungen durch Aufsichtsbehörden
Bei anstehenden Prüfungen durch die Aufsichtsbehörde ist der Datenschutzbeauftragte unverzüglich zu kontaktieren.

Schaubild:



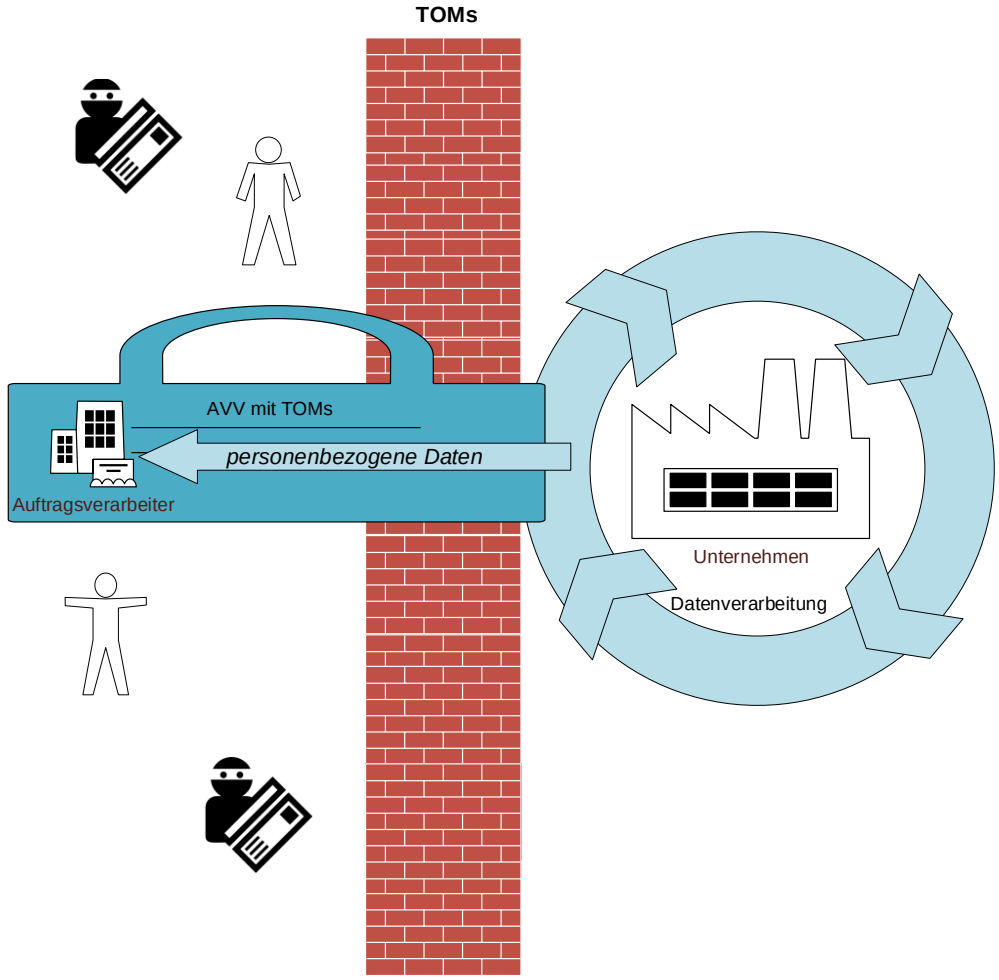
zurück

Anlage 15: Prozess Evaluierung / Verbesserung TOMs

Prozessbeschreibung:

Die technischen und organisatorischen Maßnahmen werden durch die Unternehmensleitung regelmäßig geprüft. Bei Unklarheiten ist der Datenschutzbeauftragte in die Prüfung miteinzubeziehen.

Schaubild:



zurück

Anlage 16: Prozess Sicherstellung Privacy by Design / by Default

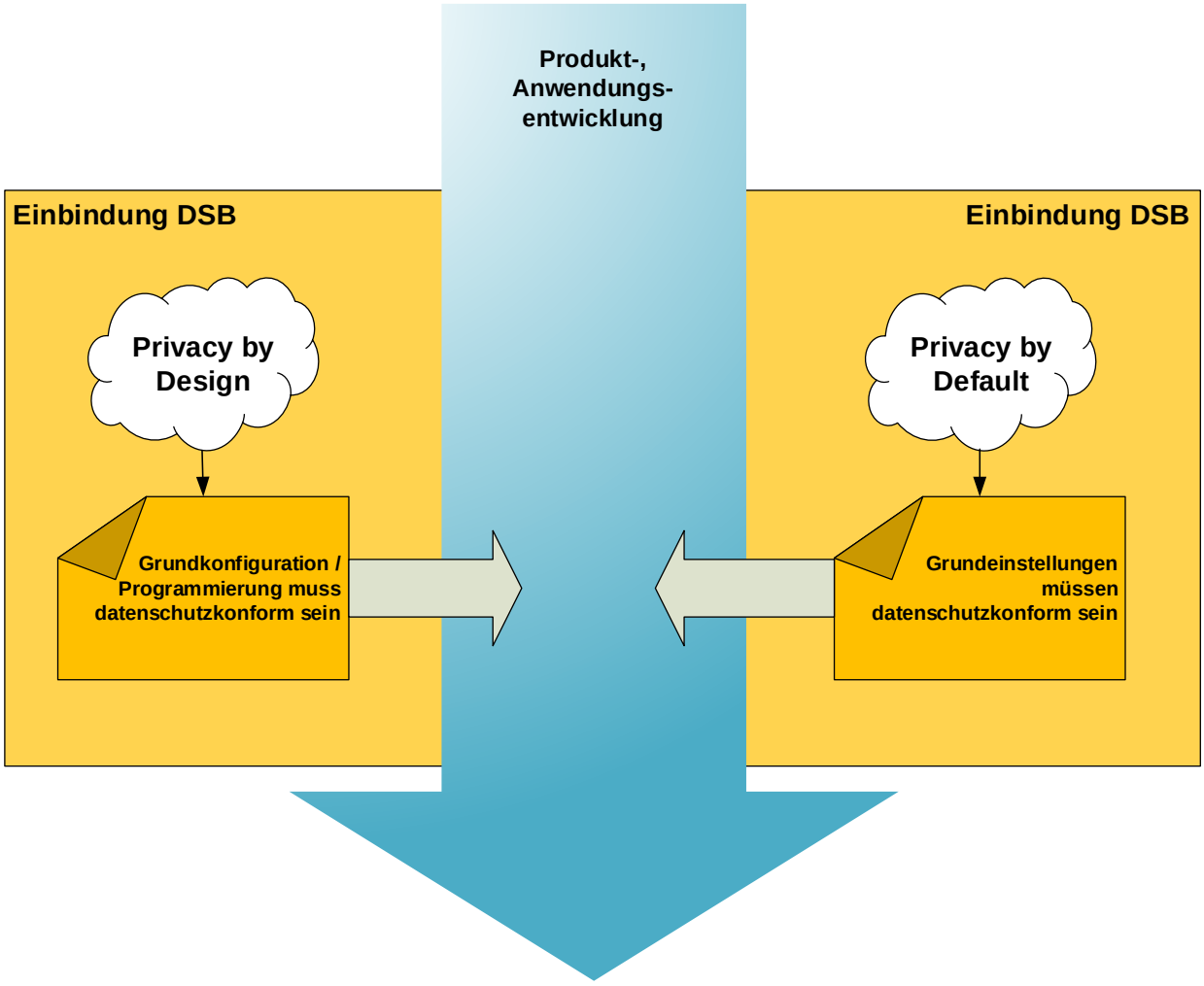
Prozessbeschreibung:

1. Beachten Sie „privacy by design“ und „privacy by default“-Grundsätze bei Einkauf und Gestaltung von IT-Lösungen!

2. Überprüfen Sie bestehende IT-Verfahren und passen Sie ggf. die inhaltliche und technische Gestaltung an!

3. Stimmen Sie Produktanforderungen mit dem Datenschutz- und IT-Sicherheitsbeauftragten ab!

Schaubild:



zurück

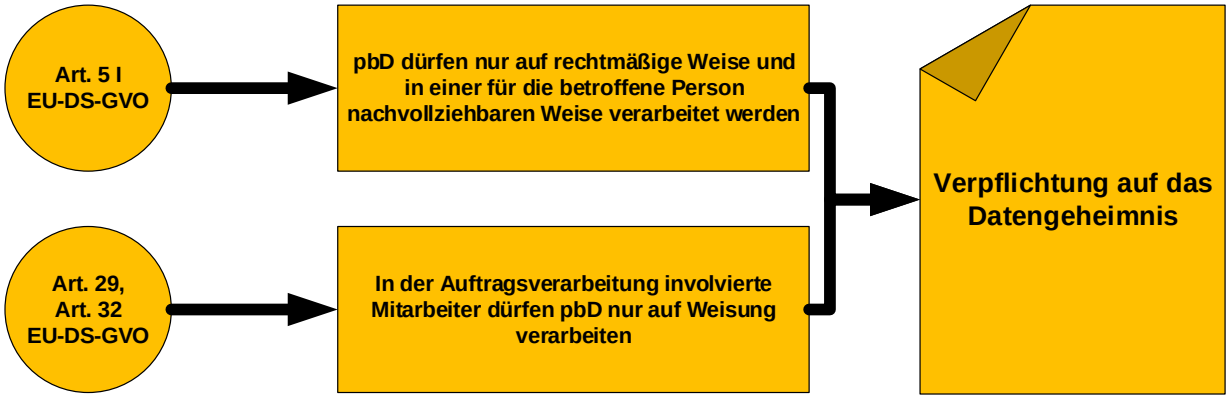
Anlage 17: Prozess Mitarbeitersensibilisierung / Verpflichtung Datenvertraulichkeit

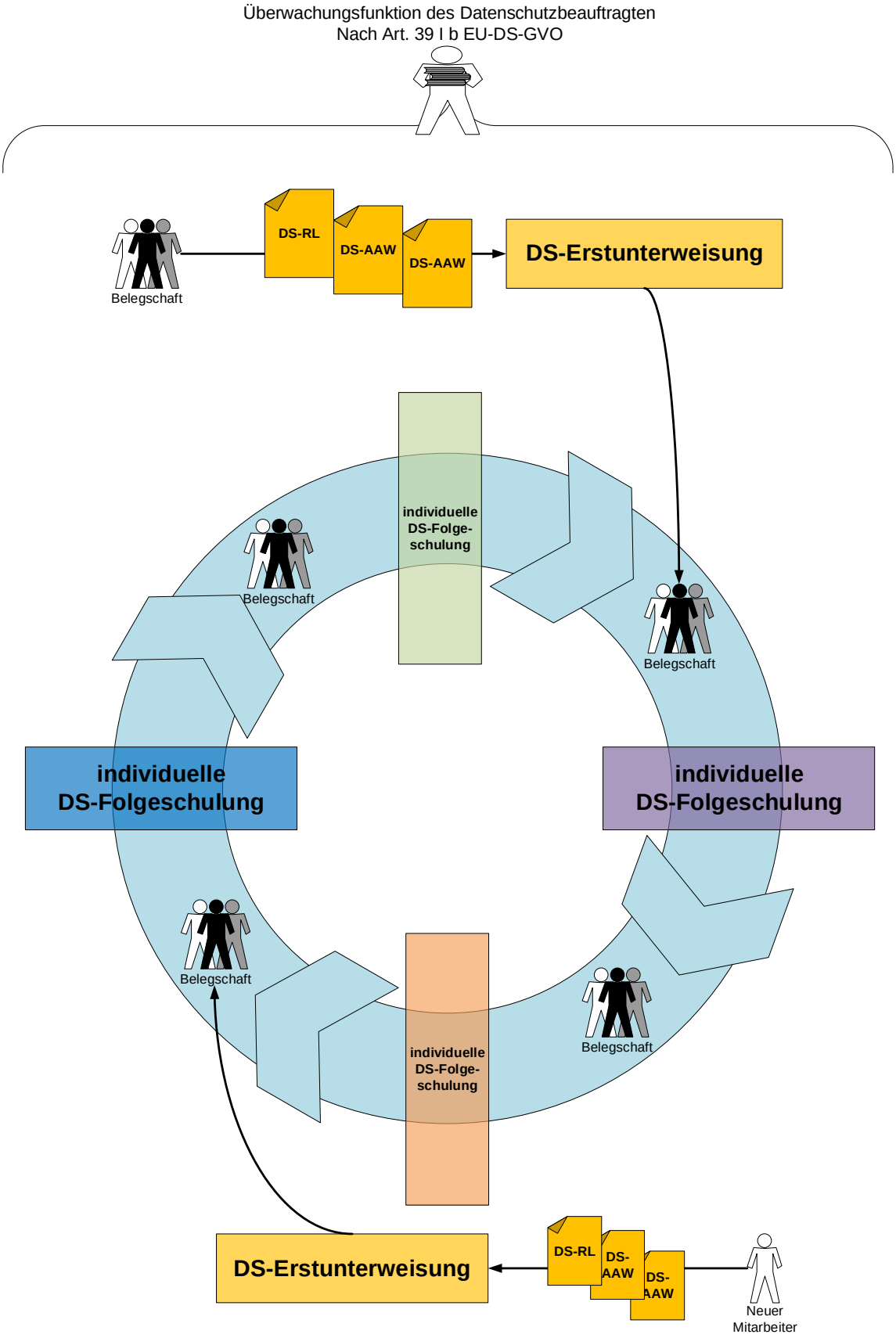
Prozessbeschreibung:

Die Mitarbeiter sind auf die Vertraulichkeit gemäß der DS-GVO verpflichtet.

Datenschutzschulungen für die Mitarbeiter finden in regelmäßigen Abständen (mindestens alle zwei Jahre) durch Frau Barbara Bucher statt. Hierbei sind auch die in dieser Richtlinie enthaltenen Prozesse zu schulen.

Schaubild:




Überwachungsfunktion des Datenschutzbeauftragten
Nach Art. 39 l b EU-DS-GVO
Belegschaft
DS-RL
DS-AAW
DS-AAW
DS-Erstunterweisung
individuelle DS-Folge-schulung
Belegschaft
Belegschaft
individuelle DS-Folgeschulung
individuelle DS-Folgeschulung
Belegschaft
Belegschaft
individuelle DS-Folge-schulung
DS-Erstunterweisung
DS-RL
DS-AAW
DS-AAW
Neuer Mitarbeiter

zurück