EU-DSGVO BEI PERSONIO

WIE WIR DIE NEUE EU-DATENSCHUTZ-GRUNDVERORDNUNG TECHNISCH UND ORGANISATORISCH UMSETZEN

Personio

01 Grundsätze
DSGVO Kapitel 2

02 Betroffenenrechte
DSGVO Kapitel 3

03 Verantwortliche & Auftragsverarbeiter
DSGVO Kapitel 4

EU-DSGVO bei Personio

Am 25.05.2018 tritt die Datenschutz-Grundverordnung (DSGVO) nach einer zweijährigen Übergangsfrist in der Europäischen Union in Kraft. Die Verordnung zielt dabei insbesondere auf den Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten sowie den freien Verkehr solcher Daten ab. Ziel ist die Harmonisierung des europäischen Datenschutzrechts. Wesentliche Änderungen der DSGVO und des neuen Bundesdatenschutzgesetzes im Vergleich zur alten Fassung sind insbesondere die Stärkung der Betroffenenrechte, welche indirekt in den Grundsätzen zur Verarbeitung personenbezogener Daten in Kapitel 2 und Kapitel 3 zu finden sind. Weiterhin wurden die Pflichten aller für die Verarbeitung personenbezogener Daten verantwortlicher Organisationen und Auftragsverarbeiter erweitert (Kapitel 4) sowie entsprechende Bußgeldrahmen für Unternehmen deutlich erhöht (Kapitel 8).

Personio als EU-DSGVO konformes Unternehmen

„Datenschutz made in Germany" lautet unser Versprechen an unsere Kunden. Als HR-Softwareanbieter ist der vertrauensvolle Umgang mit den hochsensiblen Mitarbeiterdaten ein integraler Bestandteil unserer Produktstrategie. Deshalb begrüßen wir die neue Regelung zum besseren Schutz personenbezogener Daten und arbeiten seit Bekanntmachung der gesetzlichen Veränderung intensiv daran, unsere gesamte Organisation und insbesondere unsere Softwarelösung rechtzeitig auf das Inkrafttreten der Verordnung vorzubereiten.

Wir freuen uns, Ihnen als unseren Kunden und Partnern mitteilen zu können, dass wir alle Anforderungen der EU-Datenschutz-Grundverordnung erfüllen und damit als Organisation sowie als Software konform gemäß EU-DSGVO sind.

Den detaillierten Prüfbericht unseres Datenschutzbeauftragten der Bitkom Servicegesellschaft mbH finden Sie auf unserer Datenschutz-Website im Bereich *Downloads*.

Im Folgenden möchten wir Ihnen einen tieferen Einblick in alle Maßnahmen und Veränderungen auf technischer und organisatorischer Seite geben, welche wir im Zusammenhang mit den Vorbereitungen auf die DSGVO umgesetzt haben. Wir orientieren uns dabei an der Struktur des Gesetzestextes und führen die wichtigsten Maßnahmen auf Basis der wesentlichen Artikel auf.

Inhaltsverzeichnis

01 *Grundsätze (Kapitel 2 DSGVO)*

Kapitel 2 der DSGVO legt insbesondere die Grundsätze und Rechtmäßigkeit einer Verarbeitung von personenbezogenen Daten fest (Art. 5 und 6 DSGVO). Demnach sind personenbezogene Daten beispielsweise nur auf rechtmäßige und nachvollziehbare Weise zu verarbeiten. Für die Verarbeitung von personenbezogenen Daten muss eine Rechtsgrundlage, beispielsweise die Einwilligung der Betroffenen oder eine rechtliche Verpflichtung, vorliegen. Die verantwortliche Stelle hat dabei die Einhaltung der Grundsätze im Datenschutz nachzuweisen und ist demnach rechenschaftspflichtig.

Als Auftragsverarbeiter haben wir interne Prozesse und Strukturen geschaffen mit dem Ziel, ein Datenschutz-/Informationssicherheitsmanagement-System aufzubauen, das wir kontinuierlich weiterentwickeln und so eine fortlaufende Verbesserung des Schutzes personenbezogener Daten bei Personio erwirken. Dazu haben wir im ersten Schritt ein Datenschutz- und Informationssicherheits-Team mit Mitarbeitern aus dem technischen und rechtlichen Bereich aufgestellt. Das Team kümmert sich um die Definition, Umsetzung und Prüfung von entsprechenden Konzepten und Prozessen rund um das Datenschutz- und Informationssicherheitsmanagement. Zudem haben wir die Ziele und Grundsätze im internen Datenschutz in einer zentralen Richtlinie festgehalten, welche dazu dient, allen unseren Mitarbeitern die Wichtigkeit des Themas zu verdeutlichen (Richtlinie auf Anfrage erhältlich).

02 *Maßnahmen zur Wahrung der Betroffenenrechte (Kapitel 3 DSGVO)*

Transparenz & Information (Art. 12, 13, 14 DSGVO)

- Im Rahmen der neuen DSGVO haben wir gemeinsam mit unserem Datenschutzbeauftragten eine Datenschutzerklärung für unsere Applikation ausgearbeitet. Damit kann jeder Nutzer einsehen, welche Daten von uns in eigener Verantwortung verarbeitet werden, welche Drittanbieter zur Bereitstellung der Dienstleistungen genutzt werden, wofür wir diese Daten benötigen und welche Rechte den Nutzern zustehen. **Wichtig:** Die in Personio verwalteten Personaldaten Ihres Unternehmens werden ausschließlich von den im Auftragsverarbeitungsvertrag erwähnten Unterauftragnehmern verarbeitet. Die in der Datenschutzerklärung erwähnten Drittanbieter erhalten keinerlei Zugriff auf diese Daten.
- Die Datenschutzerklärung sowie das Impressum von Personio ist innerhalb der Applikation für jeden Nutzer direkt über die Menüleiste auf der linken Seite erreichbar und sowohl in Deutsch als auch in Englisch verfügbar.
- Um sicherzustellen, dass Sie bei der Nutzung der Personio Recruiting-Funktionen Ihrer Informationspflicht gegenüber Bewerbern gerecht werden, bieten wir die Möglichkeit, eine eigene Datenschutzerklärung auf Ihrer Personio Karriereseite zu verlinken. Eine entsprechende Vorlage finden Sie hier.

Auskunftsrecht der betroffenen Person (Art. 15 DSGVO)

- Personio unterstützt Sie als Unternehmen bei der Wahrung des Auskunftsrechts gegenüber Ihren Mitarbeitern. Aufgrund des Employee-Self-Service-Ansatzes unserer Software können Mitarbeiter über ein eigenes Benutzerkonto jederzeit direkte Einsicht in ihre eigene digitale Personalakte nehmen und nachvollziehen, welche personenbezogenen Daten in Personio verarbeitet werden.
- Änderungen der digitalen Personalakte finden Sie in der Mitarbeiterhistorie. Alle wesentlichen Aktivitäten werden zudem protokolliert und für 30 Tage gespeichert, um Zugriffe und Veränderungen an Daten nachweisen zu können. Bei Unregelmäßigkeiten stellen wir Ihnen diese Protokolle auf Anfrage gerne zur Verfügung.

Recht auf Berichtigung (Art. 16 DSGVO)

- Mitarbeiter können jederzeit die unverzügliche Berichtigung unrichtiger personenbezogener Daten verlangen. Mittels der Konfiguration von Mitarbeiterrollen steht Ihnen in Personio ein umfassendes Berechtigungskonzept zur Verfügung, mit dem Sie individuell festlegen können, welche Daten Ihre Mitarbeiter einsehen oder bearbeiten dürfen.
- Über Vorschlags- und Bearbeitungsrechte können Mitarbeiter ausgewählte Personaldaten selbst verwalten und ggf. berichtigen. Ansonsten liegt es in der Verantwortung des jeweiligen Account-Administrators, der Anfrage auf Berichtigung nachzukommen.

02 *Maßnahmen zur Wahrung der Betroffenenrechte (Kapitel 3 DSGVO)*

Recht auf Löschung (Art. 17 DSGVO)

- Sobald der Zweck der Datenverarbeitung hinfällig wird, müssen Bewerber- und Arbeitnehmerdaten unter Berücksichtigung etwaiger gesetzlicher Aufbewahrungspflichten unverzüglich gelöscht werden. Dies ist beispielsweise der Fall, wenn das Beschäftigungsverhältnis eines in Personio verwalteten Mitarbeiters endet und entsprechende arbeitsrechtliche, steuerliche oder sozialversicherungsrechtliche Aufbewahrungspflichten abgelaufen sind (siehe auch Art. 18 DSGVO). In diesem Fall ermöglicht Personio eine vollständige **Löschung aller Mitarbeiterdaten** inklusive aller in Personio verwalteter Dokumente. In der **Mitarbeiterübersicht** kann dieser Vorgang für mehrere Mitarbeiter gleichzeitig vorgenommen werden.
- Personio unterstützt die vollständige Löschung von Bewerberdaten. Aktivieren Sie hierzu die automatische **Löschung von Bewerberdaten** in den Recruiting-Einstellungen. Dadurch werden alle personenbezogenen Daten von abgesagten oder abgelehnten Bewerbern nach der definierten Frist unwiederbringlich aus der Personio Applikation entfernt. Anonymisierte Metadaten der Bewerber ohne Personenbezug bleiben für Ihr Berichtswesen weiterhin erhalten.
- Im Falle der Beendigung der Geschäftsbeziehung mit der Personio GmbH können weisungsberechtigte Personen Ihres Unternehmens die Herausgabe sämtlicher Daten in einem maschinenlesbaren Format beantragen. 30 Tage nach Beendigung der Geschäftsbeziehung wird der Personio Account Ihrer Organisation und alle damit in Verbindung stehenden Daten automatisch und unwiederbringlich gelöscht, womit wir dem Recht auf Löschung nachkommen.

Recht auf Einschränkung der Verarbeitung (Art. 18 DSGVO)

Die Personalakte sollte aus arbeitsrechtlicher Sicht grundsätzlich bis zu drei Jahre über die Beendigung des Beschäftigungsverhältnisses hinaus aufbewahrt werden. Nach Art. 18 DSGVO können Ihre Mitarbeiter hierfür oder für den Fall unrichtiger Daten jedoch um eine Einschränkung der Daten bitten, um sicherzustellen, dass diese nicht unbeabsichtigt für unerwünschte Zwecke weiterverwendet bzw. verändert werden. Über das umfassende **Zugriffs- und Berechtigungskonzept** von Personio haben Sie die Möglichkeit, den Umfang der Datenverarbeitung für ehemalige Mitarbeiter individuell zu steuern.

Recht auf Datenübertragbarkeit (Art. 20 DSGVO)

- Ihre Mitarbeiter haben das Recht, sämtliche sie selbst betreffenden personenbezogenen Daten in einem strukturierten, gängigen und maschinenlesbaren Format anzufordern. Aufgrund des **Employee-Self-Service-Ansatzes** von Personio können Mitarbeiter jederzeit Einsicht in die eigene digitale Personalakte nehmen, Daten über die **Mitarbeiterübersicht** exportieren und Dokumente herunterladen.
- Support- und weisungsberechtigte Nutzer in Ihrer Organisation können ab 25. Mai 2018 einen vollständigen Unternehmensexport mit allen in Personio gespeicherten Daten in Form einer Zip-Datei durchführen.

03 *Maßnahmen für Verantwortliche & Auftragsverarbeiter (Kapitel 4 DSGVO)*

Privacy by Design & Default: Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen (Art. 25 DSGVO)

Im Rahmen der Vorbereitungen auf die EU-DSGVO wurde die gesamte Personio Applikation hinsichtlich der Voreinstellungen geprüft und angepasst, um von Anfang an ein höchstmögliches Maß an Datenschutz bei gleichzeitiger Nutzerfreundlichkeit zu gewährleisten. Hierzu zählen bspw. die standardmäßige Einschränkung von Attributen, die über unsere Personaldaten-API übergeben werden, private Kalender-Einladungen für Bewerberinterviews und Feedbackgespräche sowie die Möglichkeit, jegliche E-Mail-Benachrichtigungen für Ihren Personio Account zu deaktivieren.

- Personio Mitarbeiter haben ab 25. Mai 2018 keinen Zugriff auf Ihren Personio Account; diesen können Sie jedoch anlassbezogen für Mitarbeiter des Personio Customer Success Teams freigeben (weitere Details siehe Abschnitt „Sicherheit der Verarbeitung (Art. 32 DSGVO)“).
- Unsere Voreinstellungen sind so konzipiert, dass Sie das System nach Ihren Bedürfnissen individuell anpassen können, wie etwa durch die Konfiguration eines aggregierten Abwesenheitskalenders, der Ihren Mitarbeitern Einsicht auf die Abwesenheiten von Kollegen erlaubt, ohne jedoch die Art der Abwesenheit preiszugeben.
- Um datenschutzfreundliche Voreinstellungen und Datenschutz durch Technikgestaltung auch fortlaufend zu gewährleisten, haben wir einen Prozess definiert, um gesetzliche Anforderungen kontinuierlich in den Produktentwicklungsprozess einzuspeisen und die Anwendung in regelmäßigen Abständen zu überprüfen. Neben der verpflichtenden Kennzeichnung der Datenschutzrelevanz vor der Entwicklung neuer Funktionalitäten durch das Produktentwicklungs-Team sowie dem Zugriff des Datenschutz- und Informationssicherheits-Teams auf die kurzfristige Produkt-Roadmap sind quartalsweise Sitzungen zur Klärung neuer Fragestellungen im Bereich Datenschutz- und Informationssicherheit angedacht.

Auftragsverarbeitungsvertrag (Art. 28 DSGVO)

Wie bereits im alten Recht des Bundesdatenschutzgesetzes hat eine Auftragsverarbeitung (früher auch „Auftragsdatenverarbeitung“ oder „ADV“ genannt) stets auf Basis eines Vertrags zu erfolgen. Im Rahmen der DSGVO spricht man vom Auftragsverarbeitungsvertrag (AVV). Wir haben unseren AVV grundlegend überarbeitet und an die Anforderungen der DSGVO angepasst, insbesondere im Hinblick auf die Wahrung der Betroffenenrechte aus Kapitel 3 DSGVO sowie die Verankerung entsprechender Kontroll-, Melde- und Nachweispflichten. Eine wesentliche Erleichterung für unsere Kunden und uns als Auftragsverarbeiter ist, dass der Vertrag künftig in elektronischer Form, ähnlich wie bei unseren Nutzungsverträgen über die allgemeinen Geschäftsbedingungen, geschlossen werden kann. Damit ist eine postalische Versendung des AVV in Schriftform nicht mehr erforderlich. Der neue AVV kann ab sofort direkt in der Personio Applikation unterzeichnet werden. Im Bereich *Paket* und *Rechnung* in den *Einstellungen* finden Sie einen neuen Reiter mit der aktuellen Version. Tragen Sie einfach in die vorgesehenen Felder alle relevanten Unternehmensinformationen ein und generieren Sie Ihren individuellen Vertrag. Durch das Bestätigen der Annahmeerklärung erfolgt die digitale Unterschrift. Den unterzeichneten AVV können Sie jederzeit innerhalb der Applikation aufrufen

03 Maßnahmen für Verantwortliche & Auftragsverarbeiter (Kapitel 4 DSGVO)

und herunterladen. Wichtig ist, dass ein Vertretungsberechtigter Ihres Unternehmens die elektronische Signatur abgibt. Zudem können Sie Einsicht in die technischen und organisatorischen Maßnahmen (TOM) und die Liste der Subunternehmen nehmen sowie Weisungsberechtigte in Ihrer Organisation benennen bzw. ändern (siehe dazu auch den Abschnitt „Sicherheit der Verarbeitung"). Weitere Informationen und eine detaillierte Erklärung des Prozesses finden Sie hier.

Verzeichnis von Verarbeitungstätigkeiten (Art. 30 DSGVO)

Nach Art. 30 DSGVO muss Ihr Unternehmen als „verantwortliche Stelle" ein Verzeichnis über alle Verarbeitungstätigkeiten führen, für die es zuständig ist. Diese Anforderung gilt grundsätzlich für alle Unternehmen mit mehr als 250 Mitarbeitern. Bei Unternehmen mit weniger als 250 Mitarbeitern gelten diese nur für diejenigen Verarbeitungen, die ein Risiko für die Rechte und Freiheiten der betroffenen Personen darstellen oder nicht nur gelegentlich erfolgen. Dies ist in der Regel bei allen Prozessen im Personalwesen und Recruiting, und damit auch bei der Nutzung der Personio Applikation, der Fall. Aus diesem Grund haben wir die wesentlichen Verarbeitungstätigkeiten innerhalb der Personio Software hier zusammengestellt.

Sicherheit der Verarbeitung (Art. 32 DSGVO)

Nach Art. 32 DSGVO müssen Sie als verantwortliche Stelle und wir als Auftragsverarbeiter für die Verarbeitung personenbezogener Daten entsprechende technische und organisatorische Maßnahmen (TOM) umsetzen, welche den Stand der Technik, die Implementierungskosten und das Risiko für die Rechte und Freiheiten der Betroffenen berücksichtigen und dabei ein angemessenes Schutzniveau gewährleisten. Wir haben in diesem Zusammenhang unser Datenschutz- und Informationssicherheits-Konzept überarbeitet und zusätzliche technische und organisatorische Maßnahmen abgeleitet, die Vertraulichkeit, Integrität, Verfügbarkeit und Widerstandsfähigkeit der Systeme und Dienste sicherstellen. Unsere neuen TOM sind zukünftig direkt über die Applikation erreichbar. Die TOM wurden gemeinsam mit unserem Datenschutzbeauftragten entwickelt und von diesem geprüft. Das Prüfergebnis finden Sie auf unserer **Datenschutz-Website.**

- *Migration der Infrastruktur zu Amazon Web Services (AWS):* Um alle Anforderungen bezüglich Datenschutz und IT-Sicherheit zu gewährleisten und gleichzeitig maximale Verfügbarkeit und Stabilität unserer Software sicherzustellen, werden wir für die Bereitstellung unserer IT-Infrastruktur und Hosting-Dienste zukünftig Amazon Web Services (AWS) nutzen. Da uns das Versprechen „Datenschutz made in Germany" weiterhin sehr wichtig ist, liegen sowohl Kundendaten als auch die Personio Applikation selbst auch zukünftig ausschließlich auf Servern in Frankfurt. Detaillierte rechtliche sowie technische Informationen dazu finden Sie im separaten Dokument „IT-Infrastruktur und Einsatz von AWS bei Personio" auf unserer **Datenschutz-Website**.
- *Verschlüsselung der Kundendaten:* Um sicherzustellen, dass weder AWS noch sonstige Drittparteien Zugang zu den Kundendaten erhalten, werden alle Kundendaten ausschließlich verschlüsselt gespeichert. Der für die Verschlüsselung verwendete Master Key wird nicht auf den Servern von Amazon generiert, sondern direkt auf entsprechend gesicherten Rechnern des Infrastructure Security Teams von Personio erstellt und gespeichert. Somit kann AWS die gespeicherten Daten nicht entschlüsseln oder einsehen. Eine detaillierte Beschreibung der verwendeten Verschlüsselungstechnologie sowie

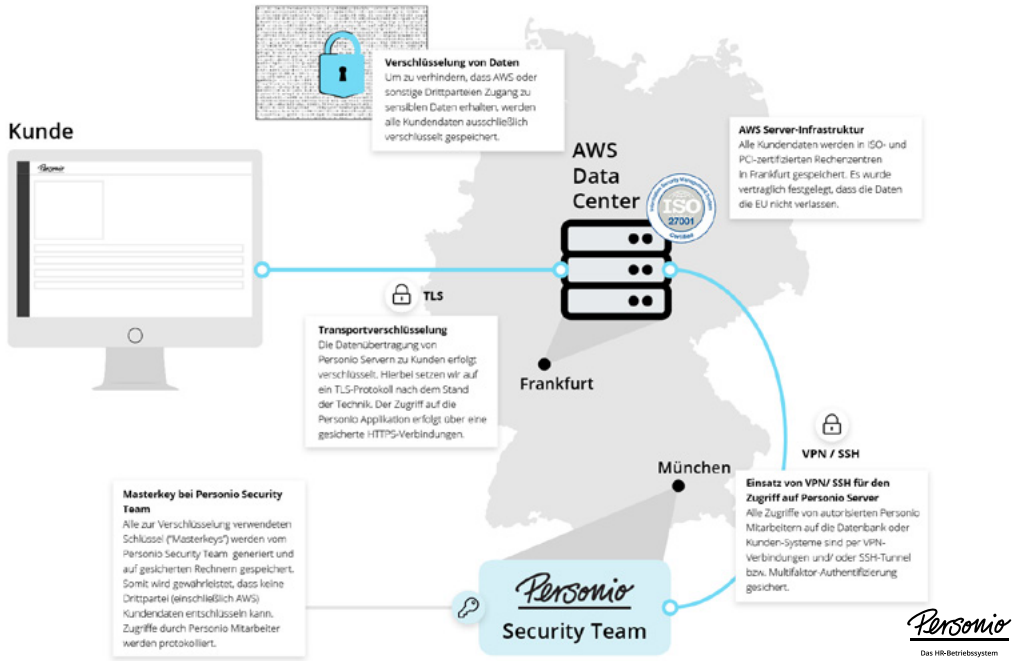
03 Maßnahmen für Verantwortliche & Auftragsverarbeiter (Kapitel 4 DSGVO)

weiterer Sicherheitsmaßnahmen finden Sie ebenfalls im Dokument „IT-Infrastruktur und Einsatz von AWS bei Personio“ auf unserer Datenschutz-Website.

- *Benennung von Support- und Weisungsberechtigten:* Um einen Missbrauch hinsichtlich der Verwaltung Ihres Kundenaccounts auszuschließen, können Sie innerhalb der Personio Applikation bis zu sieben dedizierte Weisungsberechtigte benennen. Ausschließlich die dort genannten Personen dürfen Supportanfragen stellen, den (temporären) Account-Zugriff für Personio Mitarbeiter gewähren sowie Anweisungen wie z. B. die Löschung des Kundenaccounts veranlassen. Sind keine Mitarbeiter definiert, gilt standardmäßig der Geschäftsführer als Weisungsberechtigter im Sinne der DSGVO. Die Support- und Weisungsberechtigten lassen sich in Personio innerhalb der Einstellungen unter Support definieren und jederzeit ändern.
- *Zugriffsbeschränkung auf Kundenaccount:* Personio Mitarbeiter haben ab 25. Mai 2018 keinen Zugriff auf Ihren Kundenaccount. Wenn Sie mit unseren Mitarbeitern im Customer Success in Kontakt treten wollen, um Unterstützung bei der initialen Einrichtung Ihres Accounts oder der Bearbeitung von Serviceanfragen zu erhalten, ist vorab eine Freigabe Ihres Accounts für unsere Support-Mitarbeiter notwendig. Die Zugriffsfreigabe kann nur durch zuvor festgelegte support- und weisungsberechtigte Personen in den Einstellungen unter Support gewährt und jederzeit wieder deaktiviert werden.
- *Telefon-PIN gegen Social Engineering:* Sollten Support- und Weisungsberechtigte, z.B. im Falle einer Supportanfrage, nicht identifizierbar sein, sind unsere Support-Mitarbeiter ab 25. Mai 2018 dazu angehalten, den aktuell gültigen Support-PIN abzufragen. Dies bietet einen zusätzlichen Schutz, um sicherzustellen, dass Informationen nicht versehentlich an unbefugte Anrufer weitergegeben werden können. Den Support-PIN finden Support- und Weisungsbefugte innerhalb Ihrer persönlichen Einstellungen im Bereich Support. Sie können den PIN jederzeit ändern, bspw. sofern der Verdacht besteht, dass der PIN kompromittiert wurde.
- *Erhöhte Passwortsicherheit (ab 25. Mai 2018):* Wir erhöhen die Sicherheitsanforderungen für Passwörter, die Sie und Ihre Mitarbeiter für den eigenen Personio Account vergeben können:
  - » Passwortänderungen, die mehrmals täglich erfolgen, werden blockiert
  - » Wir prüfen bereits vergebene Passwörter eines Nutzers und unterbinden diese bei der Passwortänderung
  - » Sie können festlegen, dass Mitarbeiter ihr Passwort regelmäßig aktualisieren müssen
  - » Hier finden Sie eine Übersicht aller Passwortanforderungen, die es bei der Vergabe zu berücksichtigen gilt

03 *Maßnahmen für Verantwortliche & Auftragsverarbeiter (Kapitel 4 DSGVO)*

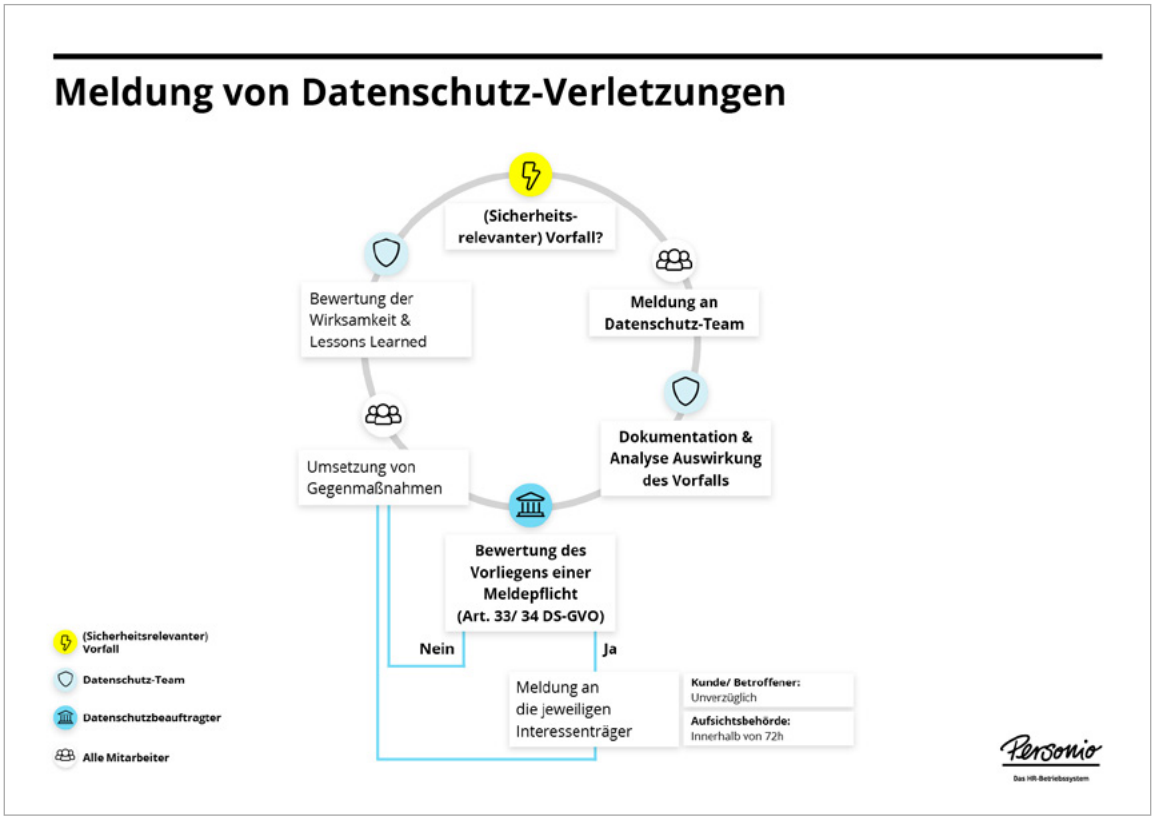
Datensicherheit bei Personio



03 *Maßnahmen für Verantwortliche & Auftragsverarbeiter (Kapitel 4 DSGVO)*

Meldung von Datenschutz-Verletzungen (Art. 33/34 DSGVO)

Im Falle einer Verletzung des Schutzes personenbezogener Daten sind Meldepflichten an die Aufsichtsbehörde zu erfüllen und die verantwortliche Stelle sowie die Betroffenen zu benachrichtigen. Zu diesem Zweck haben wir entsprechende Meldeprozesse aufgesetzt und die Berichtswege dokumentiert (siehe Abbildung).



Datenschutzbeauftragter (Art. 37/38/39 DSGVO)

Als Auftragsverarbeiter, der Verarbeitungsvorgänge von personenbezogenen Daten durchführt, sind wir seit jeher dazu verpflichtet, einen Datenschutzbeauftragten zu bestellen. Seit 01.03.2018 setzen wir auf die Dienste der Bitkom Servicegesellschaft mbH. Konkret arbeiten wir mit Herrn Tobias Göldner, langjähriger Berater im Bereich Datenschutz bei Bitkom Consult und zertifizierter Datenschutzbeauftragter (GDDCert.), zusammen (Bestellungsurkunde siehe Datenschutz-Website unter *Downloads*). Herr Göldner berät uns intensiv zu den Anforderungen der DSGVO und bringt dabei die Expertise der *Arbeitsgruppe Datenschutz* der Bitkom ein, einem der führenden Beratungsunternehmen in Deutschland rundum alle Themen aus der Digitalwirtschaft. Bei weiteren Fragen zum Thema Datenschutz bei Personio wenden Sie sich gerne an datenschutz@personio.de.

03 *Maßnahmen für Verantwortliche & Auftragsverarbeiter (Kapitel 4 DSGVO)*

Nachweis und Zertifizierung (Art. 42 DSGVO)

Die DSGVO fordert an unterschiedlichen Stellen die Erbringung eines Nachweises für Verantwortliche und Auftragsverarbeiter darüber, dass alle Pflichten, insbesondere die Umsetzung geeigneter technischer und organisatorischer Maßnahmen, erfüllt werden. Die europäischen Mitgliedsstaaten haben sich dabei selbst die Aufgabe gegeben, entsprechende Verhaltensregeln (Art. 40 DSGVO) zu definieren und ein datenschutzspezifisches Zertifizierungsverfahren (Art. 42 DSGVO) einzuführen, um einen Standard als Nachweis zu setzen. Dies ist trotz der zweijährigen Übergangsfrist bisher noch nicht erfolgt. Aus diesem Grund haben wir uns dazu entschieden, hier einen eigenen Weg zu gehen und unsere TOM (siehe oben), unser Produkt und unsere Organisation von der Bitkom Servicegesellschaft mbH auf Erfüllung der DSGVO prüfen zu lassen. Die Ergebnisse der Prüfung durch unseren Datenschutzbeauftragten finden Sie auf unserer Datenschutz-Website unter *Downloads*. Des Weiteren haben wir unsere Applikation sowie die API von einem externen und BSI-zertifizierten Dienstleister, der Secuvera GmbH, im Rahmen eines Penetrationstests testen lassen. Der Test ist positiv ausgefallen und es konnte keine kritische Schwachstelle gefunden werden. Nähere Informationen zu den Ergebnissen und der Vorgehensweise des Tests erhalten Sie gerne auf Anfrage.

Abschließend möchten wir Sie gerne auf unsere **Datenschutz-Website** unter personio.de/datenschutz hinweisen, auf der Sie weiterführende Informationen und Dokumente zum Thema einsehen bzw. anfordern können. Sollten dennoch Fragen ungeklärt bleiben, wenden Sie sich gerne an datenschutz@personio.de.

Stand: 14.05.2018

Personio

Das HR-Betriebssystem