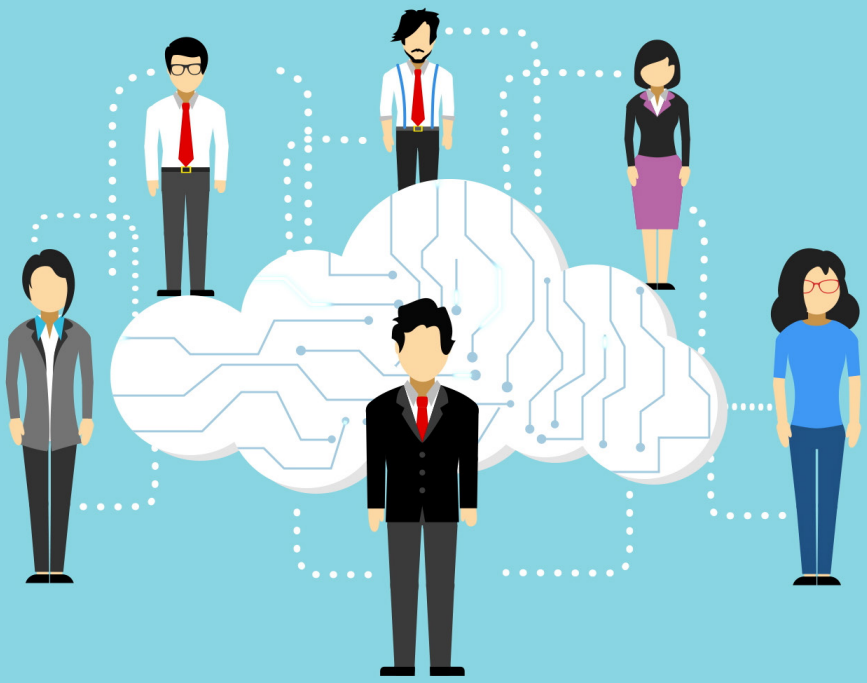

Datenverarbeitung dokumentieren: Der EDSB-Leitfaden zur Sicherstellung der Rechenschaftspflicht

Print ISBN: 978-92-9242-382-7 DOI: 10.2804/819592 QT-05-18-173-DE-C
PDF ISBN: 978-92-9242-385-8 DOI: 10.2804/350977 QT-05-18-173-DE-N

Rechenschaftspflicht vor Ort

Eine unrechtmäßige Verarbeitung von Daten kann schwerwiegende Folgen für das Leben und die Rechte der Personen haben, deren Daten wir verarbeiten. Deshalb muss der Grundsatz der Rechenschaftspflicht, der auch den Nachweis einer Einhaltung der Datenschutzvorschriften umfasst, im Mittelpunkt aller von uns durchgeführten Datenverarbeitungsvorgänge stehen.

Bei der Verarbeitung personenbezogener Daten müssen die Organe, Einrichtungen und Agenturen der EU bestimmte Vorschriften einhalten.

Wenn Sie im Namen ihres EU-Organs für die Verarbeitung personenbezogener Daten zuständig sind, tragen Sie eine Rechenschaftspflicht dafür, was Sie tun, warum Sie es tun und wie Sie es tun. Sie müssen also die Einhaltung der Datenschutzvorschriften nicht nur gewährleisten, sondern diese Einhaltung auch nachweisen können.

Eine Möglichkeit, einen solchen Nachweis zu erbringen, besteht darin, alle Verarbeitungsvorgänge in Ihrem EU-Organ zu dokumentieren. In Abhängigkeit davon, wie hoch das Risiko ist, das für die betroffene Person von einem Verarbeitungsvorgang ausgeht, müssen Sie eine oder mehrere der folgenden Dokumentationspflichten erfüllen:

- **Für alle Verarbeitungsvorgänge**: Konformitätskontrolle und Verarbeitungsverzeichnis
- **Für Verarbeitungsvorgänge mit hohem Risiko:** Datenschutz-Folgenabschätzung (DSFA)
- **Für Verarbeitungsvorgänge mit hohem Restrisiko und in Artikel 40 Absatz 4 der Verordnung aufgeführte Verarbeitungsvorgänge:** Vorherige Konsultation

Dabei kann Ihnen das Instrumentarium des EDSB zur Rechenschaftspflicht vor Ort behilflich sein.

Was ist unter Verzeichnissen zu verstehen?

Ein Verzeichnis ist die grundlegende Dokumentation, die Sie für sämtliche Verarbeitungsvorgänge erstellen müssen. Alle Verzeichnisse werden in einem von Ihrem EU-Organ geführten zentralen Register erfasst und in der Regel durch den Datenschutzbeauftragten (DSB) Ihres Organs verwaltet. Dabei ist zu beachten, dass die Verantwortung für alle von Ihnen erstellten Verzeichnisse ausschließlich bei Ihnen liegt, auch wenn der Datenschutzbeauftragte am ehesten imstande ist, dieses Register zu verwalten.

Das Verzeichnisregister sollte öffentlich zugänglich sein. Auf diese Weise kann Ihr Organ einen wirksamen und transparenten Nachweis über die Einhaltung der Datenschutzvorschriften erbringen.

Wann sollten Sie eine Datenschutz-Folgenabschätzung durchführen?

Bei einigen risikobehafteten Verarbeitungsvorgängen reicht eine Aufzeichnung allein nicht aus. Einige Beispiele:

- die Verarbeitung großer Mengen sensibler personenbezogener Daten wie Gesundheitsdaten;
- die Verarbeitung von Daten im Zusammenhang mit Disziplinarangelegenheiten;
- der Einsatz von Profiling-Verfahren.

In diesen und anderen Fällen müssen Sie eine Datenschutz-Folgenabschätzung durchführen.

Der EDSB stellt eine Vorlage zur Verfügung, die Sie bei der Durchführung einer solchen Abschätzung unterstützen soll.

Wie führen Sie eine Datenschutz-Folgenabschätzung durch?

Für eine DSFA ist eine ausführliche Analyse Ihres geplanten Verarbeitungsvorgangs erforderlich, um die damit verbundenen spezifischen Datenschutzrisiken zu ermitteln und Maßnahmen zu ihrer Abmilderung zu entwickeln. Zum Abschluss dieses Verfahrens wird ein DSFA-Bericht erstellt. Denken Sie jedoch daran, dass es sich bei DSFA um fortlaufende Verfahren handelt. Sie sollten also regelmäßige Überprüfungen einplanen.

Der EDSB stellt Vorlagen für die Durchführung von DSFA bereit, um Sie bei diesem Vorgang zu unterstützen. Es können jedoch sämtliche Methoden zum Einsatz kommen, die den Anforderungen der Verordnung oder der DSGVO entspricht.

Wann sollten Sie um eine vorherige Konsultation ersuchen?

Wenn Sie nicht sicher sind, ob die in Ihrem DSFA-Bericht ermittelten Risiken ausreichend gemildert werden konnten, müssen Sie den EDSB um die Durchführung einer vorherigen Konsultation ersuchen. In den meisten Fällen wird Ihnen der EDSB geeignete Empfehlungen vorlegen, wie sich die Einhaltung innerhalb von acht Wochen nach Eingang Ihres Ersuchens verbessern lässt.

Wie sollten Sie mit den neuen Dokumentationsvorschriften umgehen?

Da Ihr EU-Organ den Datenschutz bereits in einem gewissen Umfang dokumentiert hat, werden Sie nicht bei null anfangen müssen. Bei der Erstellung der Verzeichnisse können Sie beispielsweise die an Ihren Datenschutzbeauftragten nach der alten Verordnung übermittelten Meldungen als Grundlage verwenden.

Mit der neuen Verordnung werden weitere Änderungen eingeführt. So müssen Sie beispielsweise Ihre Unterauftragnehmer besser kontrollieren und Ihren Datenschutzhinweis aktualisieren.

Wie kann Sie Ihr Datenschutzbeauftragter unterstützen?

In jedem EU-Organ gibt es mindestens einen Datenschutzbeauftragten. Der Datenschutzbeauftragte fungiert als Bezugsperson für alle Fragen im Zusammenhang mit dem Datenschutz. In einigen größeren EU-Organen wie der Europäischen Kommission gibt es darüber hinaus Datenschutzkoordinatoren oder -Kontaktstellen. Die Datenschutzbeauftragten und Datenschutzkoordinatoren bzw. -kontaktstellen können Ihnen bei der Erstellung von Aufzeichnungen und der Durchführung von DSFA behilflich sein. Bei allen weiteren datenschutzrelevanten Fragen sollten Sie sich ebenfalls an sie wenden. Beachten Sie bitte, dass

Sie es sind, die als für die Datenverarbeitung Verantwortlicher die Einhaltung der Vorschriften

Wie kann der EDSB Ihnen helfen?

Der EDSB ist die für den Datenschutz in den EU-Organen und -Einrichtungen zuständige Aufsichtsbehörde. Unsere Aufgabe ist es, die Einhaltung der Datenschutzvorschriften durch die EU-Organe zu überwachen und zu prüfen. Dies umfasst die Untersuchung von Beschwerden, die Durchführung von Inspektionen, die Vorlage von Stellungnahmen zu vorherigen Konsultationen oder die Durchführung von Untersuchungen auf eigene Initiative. Wir formulieren Leitlinien und bieten Fortbildungen an, um Sie bei der Einhaltung der Vorschriften und der Einführung bewährter Verfahren zu unterstützen und auf diese Weise sicherzustellen, dass die EU-Organe im Bereich des Datenschutzes mit gutem Beispiel vorangehen.

Unter **personenbezogenen Daten** versteht man alle Informationen, die sich auf eine (direkt oder indirekt) identifizierbare natürliche Person beziehen. Als identifizierbar wird eine natürliche Person angesehen, die 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.

Beispiele: Name, E-Mail-Adresse, Unterlagen zur jährlichen Beurteilung, Gesundheitsakten, aber auch Informationen, die eine indirekte Identifizierung zulassen, wie Personalnummer, IP-Adresse, Verbindungsprotokolle, Faxnummer, biometrische Daten usw.

Verarbeitung bezieht sich auch auf jeden mit oder ohne Hilfe automatisierter Verfahren ausgeführten Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten wie das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, der Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung.

Beispiele: Einstellungsverfahren, Verfahren zur Gewährung von Finanzhilfen, Liste externer Sachverständiger, Veranstaltungsmanagement, Veröffentlichung von Bildern, Aufbau einer Online-Kooperationsplattform für Bürger oder Mitarbeiter.

Eine Verarbeitung findet auch statt, wenn europäische Organe oder Einrichtungen den Mitgliedstaaten ein technisches Instrument oder eine technische Lösung für den Informationsaustausch zur Verfügung stellen und weiter Zugang zu den betreffenden personenbezogenen Daten haben oder ein Register über die mit der Plattform in Zusammenhang stehenden Verbindungsprotokolle führen.

In unseren Informationsblättern erfahren Sie mehr über die neuen Datenschutzvorschriften:

- **The GDPR for EU institutions: your rights in the digital era (Die DSGVO für EU-Organe: Ihre Rechte im digitalen Zeitalter)**
- **New data protection rules for EU institutions and how they affect YOU (Wie wirken sich die neuen Datenschutzvorschriften für EU-Organe auf IHRE Arbeit aus)**

Oder besuchen Sie die Website des EDSB

Das vorliegende Informationsblatt wird durch den Europäischen Datenschutzbeauftragten (EDSB) herausgegeben. Die 2004 eingerichtete unabhängige EU-Behörde

- überwacht die Verarbeitung personenbezogener Daten durch EU-Organe und -Einrichtungen;
- berät zu Rechtsvorschriften zum Datenschutz;
- arbeitet mit vergleichbaren Behörden zusammen, um einen kohärenten Datenschutz sicherzustellen.

QT-05-18-173-DE-N

www.edps.europa.eu


@EU_EDPS


EDPS


European Data Protection Supervisor

ISBN: 978-92-9242-385-8