EVERSHEDS SUTHERLAND

Schritt für Schritt

So stellen Sie sicher, dass Ihr Unternehmen den Anforderungen der DSGVO entspricht

Die DSGVO erfordert eine gänzlich neue Herangehensweise an Verarbeitung und Schutz personenbezogener Daten. Datenschutz und der Grundsatz der Daten-Minimierung müssen Eingang in alle Unternehmensbereiche und -prozesse finden.

1 Definieren eines Projektteams

- Bestimmen Sie, wer in Ihrem Unternehmen für die Einhaltung der DSGVO verantwortlich ist und stellen Sie ein internes Compliance -Team auf
- Legen Sie fest, ob die Strategie zur Erreichung zukünftiger DSGVO-Compliance auf Konzernebene oder jeweils innerhalb der einzelnen Konzerngesellschaften festgelegt und verfolgt wird
- Stellen Sie sicher, dass die Unternehmensleitung die erforderlichen Ressourcen für das Compliance-Projekt bewilligt
- Legen Sie fest, welcher Ihrer Standorte in der EU Ihre Hauptniederlassung hinsichtlich Datenschutz-Fragen sein soll

2 Datenmapping

- Erheben Sie, welche personenbezogenen Daten wie und wofür im Unternehmen verarbeitet werden und bilden Sie die bestehenden Verarbeitungsprozesse ab
- Dokumentieren Sie die Verarbeitungsvorgänge, für die Sie verantwortlich sind, schriftlich
- Aktualisieren Sie Ihren Umsetzungsplan, nachdem Sie ihn mit Ihren Ergebnissen zum Datenmapping abgeglichen haben

3 Lückenanalyse

- Analysieren Sie alle Unternehmensrichtlinien, Arbeitsabläufe und Datenverarbeitungstätigkeiten hinsichtlich der Anforderungen der DSGVO
- Evaluieren Sie die Compliance-Risiken, denen Ihr Unternehmen ausgesetzt ist
- Präsentieren Sie der Unternehmensleitung einen Bericht, der alle Compliance-Lücken sowie Optionen zur Schadensbehebung aufzeigt (z.B. Details zu den voraussichtlich erforderlichen Ressourcen, Zeitaufwand und Dringlichkeitsstufe)
- Priorisieren Sie bei der Umsetzung von Lösungen die Bereiche mit dem höchsten Risiko
- Beziehen Sie Hinweise lokaler und überregionaler Datenschutzbehörden sowie der Artikel-29-Datenschutz-gruppe mit ein, sobald diese verfügbar werden

4 Datenschutzbeauftragter

Prüfen Sie, ob die Ernennung eines Datenschutz-beauftragten erforderlich ist. Dabei ist zu beachten, dass aus nationalem Datenschutzrecht über die DSGVO hinausgehende Benennungspflichten folgen können. Ein Datenschutzbeauftragter muss nach der DSGVO grundsätzlich benannt werden von:

- öffentlichen Behörden
- nicht-öffentlichen Stellen, sofern deren Kerntätigkeit entweder in der Durchführung von Verarbeitungs-vorgängen, welche aufgrund ihrer Art, ihres Umfangs und/ oder ihrer Zwecke eine regelmäßige und systematische Überwachung von Betroffenen erforderlich machen, oder in der umfangreichen Verarbeitung besonderer Kategorien von Daten oder personenbezogenen Daten über strafrechtliche Verurteilungen und Straftaten besteht

5 Verträge mit Auftragsverarbeitern

- Überprüfen Sie die Verträge mit Lieferanten und Dienstleistern, und verhandeln Sie diese erforderlichen-falls neu, um sicherzustellen, dass alle von der DSGVO vorgeschriebenen Bedingungen für Auftragsverarbeiter auf angemessene Weise abgedeckt sind
- Stellen Sie sicher, dass alle neuen Verträge mit Ihren Lieferanten und Dienstleistern DSGVO konform gestaltet werden
- Prüfen Sie, wie Sie Due Diligence-Prüfungen von Lieferanten und Dienstleistern durchführen und erstellen Sie entsprechende Prüflisten sowie Unterlagen zum Nachweis
- Prüfen Sie die Auswirkungen der DSGVO auf andere Klauseln in Ihren Verträgen (z.B. Haftungen)

6 Datenschutzdokumentation

- Aktualisieren Sie bestehende und erstellen neue Unternehmensrichtlinien, um Compliance-Lücken zu schließen, die während der Lückenanalyse entdeckt wurden
- Das sind z.B. Mitteilungen über faire Verarbeitung, Einwilligungserklärungen, Richtlinien zur Aufbewahrung von Unterlagen, Richtlinien für Zugriffsanfragen von Betroffenen, Datenschutzrichtlinien etc.

7 Implementieren von Prozessen

- Sorgen Sie für Einführung und Verankerung des Datenschutzes durch Gestaltungsvorgaben und Datenschutzfolgenabschätzungen
- Aktualisieren Sie die Abläufe zur Erfüllung von Betroffenenrechten (z.B. Zugriffs-, Datenportabilitäts- und. Berichtigungsanfragen, Widersprüche)
- Aktualisieren Sie die Verfahren bei Sicherheitsverstößen
- Simulieren Sie mögliche Szenarien bei Sicherheitsverstößen

8 Schulungen

- Schulen Sie gezielt Entscheidungsträger und Projektteams
- Stellen Sie sicher, dass alle Mitarbeiter angemessen für ihre Verantwortungsbereiche geschult werden

Strafdrohung

Unternehmen, die die Bestimmungen der DSGVO verletzen, riskieren Strafen bis zu 4% des jährlichen weltweiten (Konzern-) Umsatzes oder 20 Mio. EUR

Für weitere Informationen kontaktieren Sie bitte:

Dr. Georg Röhsner
Partner

georg.roehsner@ eversheds-sutherland.at

Mag. Manuel Boka
Principal Associate

manuel.boka@ eversheds-sutherland.at

Grundsätze

Wesentliches zur Datenschutz-Grundverordnung (DSGVO)

Grundprinzipien

Anwendungsbereich: Die DSGVO gilt für Organisationen, die:

- personenbezogene Daten als Verantwortlicher oder Auftragsverarbeiter im Rahmen der Tätigkeiten einer Niederlassung in der EU verarbeiten, unabhängig davon, ob die tatsächliche Datenverarbeitung innerhalb der EU stattfindet
- personenbezogene Daten als Auftragsverarbeiter für einen Verantwortlichen, auf den die DSGVO anwendbar ist, selbst wenn sich die Niederlassung und der Ort der Verarbeitung außerhalb der EU befinden
- personenbezogene Daten von Personen, die sich in der EU befinden, durch einen nicht in der EU niedergelassenen Verantwortlichen oder Auftragsverarbeiter verarbeiten, wenn die Datenverarbeitung dazu erfolgt, um

  (a) ihnen Waren oder Dienstleistungen anzubieten, unabhängig davon ob von diesen eine Zahlung zu leisten ist oder (b) das Verhalten dieser Personen in der EU zu beobachten.

One-stop-shop: Wenn eine Organisation mehr als eine Niederlassung in der EU hat, besteht die Möglichkeit, dass unter gewissen Voraussetzungen nur eine einzelne Datenschutzbehörde als „Federführende Aufsichtsbehörde" für die grenzüberschreitenden Datenverarbeitungen dieser zuständig ist.

Rechenschaftspflicht: Verantwortliche sind für die Einhaltung der Regeln hinsichtlich der Grundsätze der Datenverarbeitung verantwortlich, und müssen dies auch beweisen können.

Einwilligung:: Die Einwilligung muss durch eine eindeutige Handlung erfolgen, mit der für den konkreten Fall unmissverständlich bekundet wird, dass die betroffene Person mit der Verarbeitung der sie betreffenden personenbezogenen Daten einverstanden ist. Konkludente Einwilligungen oder bereits vorangekreuzte Einwilligungsfelder sind nicht mehr ausreichend.

Datenminimierung: Personenbezogen Daten müssen dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein.

Verpflichtungen der Auftragsverarbeiter: Auftragsverarbeitern werden durch die DSGVO direkt Pflichten auferlegt, wenn sie im Auftrag von Verantwortlichen tätig werden, insbesondere hinsichtlich Datensicherheit, internationale Datenübermittlungen, die Ernennung von Subauftragsverarbeitern und die Benachrichtigung nach der Verletzung des Schutzes personenbezogener Daten (Sicherheitslücken).

Internationale Datenübermittlungen: Die DSGVO normiert neue Sicherheitsvorkehrungen für den Datentransfer außerhalb des EWRs, insbesondere:

- Verbindliche interne Datenschutzvorschriften (binding corporate rules)
- Von Aufsichtsbehörden genehmigte Standardvertragsklauseln (standard contractual rules)
- Genehmigte Verhaltensregeln (approved codes of conduct)
- Genehmigte Zertifizierungsverfahren

Rechte betroffener Personen

Auskunftsrechte: Betroffene Personen haben das Recht auf Zugang zu einer Vielzahl an Informationen, insbesondere hinsichtlich:

- der Sicherheitsvorkehrungen, die der Verantwortliche für den internationalen Datentransfer getroffen hat
- des Zeitraums für den die gesammelten Daten voraussichtlich gespeichert werden.

In den meisten Fällen müssen Anfragen sofort, spätestens aber innerhalb eines Monats beantwortet werden. Solange die Anfrage nicht offenkundig unbegründet oder exzessiv ist, muss diese kostenlos bearbeitet werden.

Löschung: Personenbezogene Daten müssen unverzüglich gelöscht werden, sobald

- die Verarbeitung dieser nicht mehr notwendig ist;
- die Einwilligung zurückgezogen wird, und es keine weitere Rechtsgrundlage für eine Verarbeitung gibt;
- die betroffene Person Widerspruch gegen eine Verarbeitung einlegt, und keine vorrangig berechtigten Gründe für die weitere Verarbeitung vorliegen;
- sie unrechtmäßig verarbeitet wurden;
- die Löschung zur Erfüllung anderer rechtlicher Verpflichtungen erforderlich ist.

Recht auf Datenübertragbarkeit: Wenn personenbezogene Daten von einer betroffenen Person zur Verfügung gestellt wurden, und die Verarbeitung automatisiert mit Einwilligung der Person durchgeführt wurde, oder wenn sie für die Erfüllung eines Vertrages notwendig ist, ist ein Verantwortlicher dazu verpflichtet, auf Anfrage einer betroffenen Person die sie betreffenden relevanten personenbezogenen Daten an diese in einem strukturierten, gängigen und maschinenlesbaren Format zu übermitteln.

Automatisierte Entscheidungsfindung und Profiling: Betroffene Personen haben das Recht, keiner Entscheidung zur Bewertung von sie betreffenden persönlichen Aspekten unterworfen zu werden, die ausschließlich auf einer automatisierten Verarbeitung beruht, und die rechtliche Wirkungen für diese entfaltet oder sie sonst erheblich beeinträchtigt (z.B. Online-Kreditanträge oder Online-Einstellungsverfahren)

Recht auf Berichtigung: Betroffene Personen haben das Recht von dem Verantwortlichen unverzüglich die Berichtigung sie betreffender unrichtiger personenbezogener Daten zu verlangen.

Beschränkungen der Verarbeitung: Betroffene Personen können die Verarbeitung von Daten beschränken, wenn:

- die Richtigkeit der personenbezogene Daten von der Person bestritten wird. In diesem Fall gilt die Beschränkung für einen Zeitraum, der es dem Verantwortlichen ermöglicht, die Richtigkeit zu überprüfen
- die Verarbeitung unrechtmäßig ist und die betroffene Person die Löschung der personenbezogenen Daten ablehnt und stattdessen die Einschränkung der Nutzung der personenbezogenen Daten verlangt
- der Verantwortliche die personenbezogenen Daten für die Zwecke der Verarbeitung nicht länger benötigt, die betroffene Person sie aber zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen benötigt
- die betroffene Person Widerspruch gegen die Verarbeitung gemäß dem von der DSGVO eingeräumten Widerspruchsrecht eingelegt hat. Hier dauert die Beschränkung solange als noch nicht feststeht, ob die berechtigten Gründe des Verantwortlichen gegenüber denen der betroffenen Person überwiegen.

Widerspruchsrecht: Personen haben das Recht aus Gründen, die sich aus ihrer besonderen Situation ergeben, jederzeit gegen die Verarbeitung der sie betreffenden personenbezogenen Daten Widerspruch einzulegen. Der Verantwortliche darf diese dann nicht mehr verarbeiten, es sei denn, er kann zwingende schutzwürdige Gründe vorweisen, die die Interessen, Rechte und Freiheiten der betroffenen Person überwiegen.

Formvorschriften

Privacy by design: Ein Verantwortlicher muss, sobald die Mittel und der Zeitpunkt der Verarbeitung feststehen, technische und organisatorische Maßnahmen durchführen, welche derart gestaltet sind, dass sie:

- die Datenschutzprinzipien (z.B. Datenminimierung) verwirklichen
- die notwendigen Sicherheitsvorkehrungen treffen, um den Anforderungen der DSGVO gerecht zu werden und die Rechte der betroffenen Personen zu schützen.

Bestellung eines Auftragsverarbeiters: Unternehmen dürfen nur Auftragsverarbeiter betrauen, die angemessene Garantien dafür bieten, dass die Verarbeitung den Anforderungen der DSGVO entspricht, und dass jede Datenverarbeitung durch diese entweder auf Grundlage eines Vertrages oder eines anderen bindenden Rechtsinstruments erfolgt, welches sicherstellt, dass auch diese die beschriebenen Vorschriften einhalten. Dazu dürfen Auftragsverarbeiter keinen weiteren Auftragsverarbeiter (z.B. Unterauftragsverarbeiter) ohne vorherige gesonderte oder allgemeine schriftliche Genehmigung des Verantwortlichen in Anspruch nehmen.

Benachrichtigung nach einer Sicherheitslücke: Im Falle einer Sicherheitslücke und daraus folgender Verletzung des Schutzes personenbezogener Daten müssen Verantwortliche:

- die Datenschutzbehörde unverzüglich, jedenfalls jedoch innerhalb von 72 Stunden nach Kenntnis der Lücke, sowie
- die betroffenen Personen, bei denen die Verletzung wahrscheinlich ein hohes Risiko für ihre Rechte und Freiheiten mit sich bringen, unverzüglich nach Kenntnis der Lücke verständigen.

Datenschutz-Folgenabschätzung: Datenschutz-Folgenabschätzungen müssen durchgeführt werden, wenn eine Art der Verarbeitung (insbesondere bei neuen Technologien) wahrscheinlich zu einem hohen Risiko für Rechte und Freiheiten natürlicher Personen führen würde.

eversheds-sutherland.at