Richtlinie zur Umsetzung von Datenschutzmaßnahmen

Einleitung

Bei der **w3 GmbH** werden personenbezogene Daten verarbeitet. Die **w3 GmbH** ist gesetzlich verpflichtet, personenbezogene Daten unter Einhaltung der jeweils geltenden datenschutzrechtlichen Vorschriften zu verarbeiten.

Einschlägige Rechtsvorschriften sind dabei die Datenschutz-Grundverordnung (DSGVO), das Bundesdatenschutzgesetz sowie ggf. bereichsspezifische Rechtsvorschriften.

Jeder Geschäftsprozess, der mit einer Verarbeitung personenbezogener Daten einhergeht, ist von der w3 GmbH auf die Einhaltung der rechtlichen Vorgaben zu prüfen.

Zudem ist der **Datenschutzbeauftragte** der **w3 GmbH** für die Überprüfung der Einhaltung der gesetzlichen Aufgaben zuständig.

Um die Rechtskonformität von Datenverarbeitungen im Unternehmen zu gewährleisten, macht die w3 GmbH durch diese Richtlinie Vorgaben für die Einrichtung, Prüfung und Durchführung von Datenverarbeitungsprozessen. Zudem wird mit dieser Richtlinie die Erstellung und Pflege des Verzeichnisses von Verarbeitungstätigkeiten i.S.d. Art. 30 DSGVO unterstützt. Gleiches gilt für die Unterstützung im Zusammenhang mit der Prüfung, ob (und erforderlichenfalls wie) Datenschutz-Folgenabschätzungen i.S.d. Art. 35 DSGVO durchzuführen sind.

Ferner sind von der w3 GmbH etwaige Meldeüflichten nach Art. 33, 34 DSGVO einzuhalten.

Geltungsbereich

Diese Richtlinie gilt für die Beschäftigten, die für die Einrichtung oder Durchführung von Verarbeitungen personenbezogener Daten bei der w3 GmbH oder für eine Verarbeitung selbst als „Owner“/Eigentümer verantwortlich sind.

Diese Richtlinie gilt für alle Standorte der w3 GmbH.

Ziele

Diese Richtlinie soll dazu beitragen, dass die Rechtsvorschriften zur Verarbeitung personenbezogener Daten eingehalten werden.

Grundsätze für die Einrichtung oder Änderung von

Verarbeitungen personenbezogener Daten

Bei der Verarbeitung personenbezogener Daten und auch bei der Einrichtung oder Änderung von den damit zusammenhängenden Prozessen sind folgende Grundsätze der Datenverarbeitung i.S.d. Art. 5 DSGVO einzuhalten:

Personenbezogene Daten müssen

1. auf Basis einer Rechtsgrundlage oder Einwilligung, nach Treu und Glauben und in einer für die betroffene Person nachvollziehbaren Weise verarbeitet werden („Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz“);
2. für festgelegte, eindeutige und legitime Zwecke erhoben werden und dürfen nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise weiterverarbeitet werden („Zweckbindung“);
3. dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein („Datenminimierung“);
4. sachlich richtig und erforderlichenfalls auf dem neuesten Stand sein; es sind alle angemessenen Maßnahmen zu treffen, damit personenbezogene Daten, die im Hinblick auf die Zwecke ihrer Verarbeitung unrichtig sind, unverzüglich gelöscht oder berichtigt werden („Richtigkeit“);
5. in einer Form gespeichert werden, die die Identifizierung der betroffenen Personen nur so lange ermöglicht, wie es für die Zwecke, für die sie verarbeitet werden, erforderlich ist („Speicherbegrenzung“);
6. in einer Weise verarbeitet werden, die eine angemessene Sicherheit der personenbezogenen Daten gewährleistet, einschließlich Schutz vor unbefugter oder unrechtmäßiger Verarbeitung und vor unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung oder unbeabsichtigter Schädigung durch geeignete technische und organisatorische Maßnahmen („Integrität und Vertraulichkeit“);
7. für jeden Geschäftsprozess, der die Verarbeitung personenbezogener Daten beinhaltet, muss es einen Verantwortlichen bei der w3 GmbH geben („Owner/Eigentümer“)

Bei Fragen zur Anwendung und Auslegung dieser Grundsätze kann sich jeder Beschäftige an den Datenschutzbeauftragten und/oder das Datenschutzteam (DST) wenden.

Ausnahmen

Die w3 GmbH kann Ausnahmen von den unter Ziff. 4 genannten Grundsätzen in begründeten Fällen erlauben. Ausnahmen sind vom DST zu prüfen und mit der Unternehmensleitung abzustimmen. Genehmigte Ausnahmen sind inklusive einer Begründung zu dokumentieren.

Verzeichnis von Verarbeitungstätigkeiten

Die w3 GmbH führt ein Verzeichnis von Verarbeitungstätigkeiten und – soweit die w3 GmbH als Auftragsverarbeiter tätig ist – auch ein Verzeichnis von Verarbeitungstätigkeiten für Auftragsverarbeiter i.S.d. Art. 30 Abs. 2 DSGVO.

Das Verzeichnis von Verarbeitungstätigkeiten wird vom DST geführt. Das DST kann ein DST-Mitglied als federführende Person für die Pflege des Verarbeitungsverzeichnisses bestimmen. Das DST trägt

Sorge dafür, dass die Verarbeitungsverzeichnisse regelmäßig aktualisiert werden.

Alle Beschäftigten, die für die Einrichtung oder Durchführung von Verarbeitungen personenbezogener Daten bei der w3 GmbH oder für eine Verarbeitung selbst als „Owner/Eigentümer“ verantwortlich sind, sind bei einer geplanten Einrichtung oder Änderung von Verarbeitungen und/oder Geschäftsprozessen verpflichtet, dieses dem DST mitzuteilen. Die Mitteilung erfolgt per E-Mail an das DST bzw. die DST-Mitglieder.

Datenschutz-Folgenabschätzung

Das DST wird jeden neuen, gemeldeten Verarbeitungsprozess dahingehend prüfen, ob damit voraussichtlich ein hohes Risiko für personenbezogene Daten einhergeht. Gleiches gilt für die Veränderung von Verarbeitungsprozessen. Wenn ein voraussichtlich hohes Risiko besteht, wird das DST der Unternehmensleitung die Durchführung einer Datenschutz-Folgenabschätzung (DSFA) empfehlen. Die Unternehmensleitung entscheidet über das „Ob“ und „Wie“ der Durchführung der DSFA.

Die jeweilige Verarbeitung darf grundsätzlich erst nach Durchführung der DSFA und entsprechender Freigabe durch die Unternehmensleitung begonnen werden.

Die DSFA kann vom DST durchgeführt werden. Die DSFA kann auch durch externe, fachkundige Personen durchgeführt werden. Der Datenschutzbeauftragten (DSB) steht bei der Durchführung der DSFA auf Anfrage für die Beratung zur Verfügung.

Das Ergebnis der DSFA wird der Unternehmensleitung mitgeteilt. Die Unternehmensleitung entscheidet über die Freigabe des Verarbeitungsprozesses.

Sollte die DSFA ergeben, dass das mit dem Verarbeitungsprozess verbundene Risiko nicht durch technische und organisatorische Maßnahmen eingedämmt werden kann, wird die Unternehmensleitung darüber entscheiden, ob die eine vorherige Konsultation mit der Aufsichtsbehörde i.S.d. Art. 36 DSGVO durchzuführen ist.

Meldepflichten bei Datenschutzverletzungen

Das Datenschutz- und Informationssicherheitsteam (DST) untersucht unverzüglich jeden Vorfall oder jede Meldung („Vorfälle“) einer Verletzung des Schutzes personenbezogener Daten.

Jeder Vorfall wird vom DST in Textform dokumentiert. Dabei werden Zeitpunkt der Kenntnisnahme, Sachverhaltsdarstellung und getroffene Maßnahmen dokumentiert. Bei jedem Vorfall ist zunächst zu prüfen, ob eine Verletzung des Schutzes personenbezogener Daten vorliegt und die Verletzung voraussichtlich zu einem Risiko für die Betroffenen führt. Im Falle eines Risikos muss das DST unverzüglich die Unternehmensleitung informieren und Sorge dafür tragen, dass binnen 72 Stunden nach Kenntnis von dem Vorfall eine Meldung an die für die w3 GmbH zuständige Aufsichtsbehörde für den Datenschutz erfolgt.

Sollte die Frist von 72 Stunden bereits verstrichen sein, wird gleichwohl so schnell wie möglich eine Meldung an die Aufsichtsbehörde erfolgen. Dieser Meldung ist dann eine Begründung für die Verzögerung beizufügen. Die Meldung ist mit der Unternehmensleitung vorab abzustimmen.

Die Meldung muss insbesondere beinhalten:

- eine Beschreibung der Art der Verletzung des Schutzes personenbezogener Daten, soweit möglich mit Angabe der Kategorien und der ungefähren Zahl der betroffenen Personen, der betroffenen Kategorien und der ungefähren Zahl der betroffenen personenbezogenen Datensätze;
- den Namen und die Kontaktdaten des Datenschutzbeauftragten oder einer sonstigen Anlaufstelle für weitere Informationen;
- eine Beschreibung der wahrscheinlichen Folgen der Verletzung des Schutzes personenbezogener Daten;
- eine Beschreibung der von dem Verantwortlichen ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung des Schutzes personenbezogener Daten und gegebenenfalls Maßnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen.

Sollten die genannten Informationen nicht binnen der 72-Stunden-Frist ermittelt oder zusammengestellt werden können, hat gleichwohl eine Meldung an die Aufsichtsbehörde zu erfolgen. Die o.g. Inhalte sind dann unverzüglich an die Aufsichtsbehörde nachzureichen.

Wenn die Verletzung des Schutzes personenbezogener Daten voraussichtlich ein hohes Risiko für von dem Vorfall Betroffenen hat, so benachrichtigt das DST die betroffenen Personen unverzüglich von der Verletzung. Das DST wird die Meldungen vorab mit der Unternehmensleitung abstimmen und dabei insbesondere etwaige Ausnahmeregelungen nach Art. 34 Abs. 3 DSGVO in Erwägung ziehen.

Sofern die w3 GmbH personenbezogene Daten im Autrag anderer Unternehmen oder Organisationen verarbeitet, ist eine Meldung eines Vorfalls unverzüglich an den Auftraggeber der Datenverarbeitung vorzunehmen. Bezüglich Zeitpunkt und Art der Meldung ist sofort nach Kenntnis von einem Vorfall im betreffenden Auftragsverarbeitungsvertrag mit dem Auftraggeber nachzusehen, wann und wie die Meldung an den Auftraggeber zu erfolgen hat.

Schulungsmaßnahmen

Alle Beschäftigten der w3 GmbH sind zeitnah nach Beginn der Aufnahme ihrer Tätigkeit für die w3 GmbH und sodann regelmäßig (mindestens jährlich) in Datenschutzschulungen mit den Rechtsvorschriften zur Verarbeitung personenbezogener Daten vertraut zu machen.

Alle Beschäftigten, die für die Einrichtung oder Durchführung von Verarbeitungen personenbezogener Daten bei der w3 GmbH verantwortlich sind, tragen Sorge dafür, dass alle Beschäftigten, die über diese Verarbeitungen Zugang zu personenbezogenen Daten haben, zuvor zum Datenschutz geschult wurden.

Das DST wird ein Schulungskonzept entwickeln, dass die richtlinienkonforme Schulung der Beschäftigten gewährleistet, und der Unternehmensleitung vorlegen. Die Unternehmensleitung wird über die Durchführung des Schulungskonzeptes entscheiden und geeignete Schulungsmaßnahmen anordnen.

Sanktionen

Ein Verstoß gegen diese Richtlinien kann eine arbeitsvertragliche Pflichtverletzung darstellen und

entsprechend sanktioniert werden.