Basis-Orientierungshilfe für Verarbeitungsverantwortliche* in der UW/H

Das kleine „Datenschutz-3x3“

L

Legalisiere!

Machen Sie Ihre Verarbeitung rechtskonform!

- Rechtsgrundlage bestimmen[1]
- Datenschutz-Grundsätze erfüllen[2]
- Sicherheitsmaßnahmen (TOM) vorsehen[3]

D

Dokumentiere!

Erfüllen Sie die Nachweispflichten!

- Verzeichniseintrag (VVT) erstellen[4]
- AV/GV Verträge archivieren[5]
- Risikoanalyse/DSFA belegen[6]

I

Informiere!

Halten Sie die Betroffenen auf dem Laufenden!

- Datenschutzinfos vorab bereitstellen[7]
- Auskunft (und weitere Rechte) ermöglichen[8]
- Datenpannen mitteilen[9]

[1] Art. 6, Art. 9
[2] Art. 5, Art. 25
[3] Art. 32

[4] Art. 30
[5] Art. 26, Art. 28
[6] Art. 35

[7] Art. 13, Art. 14
[8] Art. 15 bis Art. 21
[9] Art. 33, Art. 34 (alle Artikel aus DSGVO)

***Verarbeitungsverantwortliche**
meint alle Personen oder Stellen, die eine Verarbeitung personenbezogener Daten im Namen und in der Verantwortung der UW/H gGmbH betreiben. In der Regel also Personen in der Rolle Lehrstuhlinhaber:in, Institutsleiter:in oder Fachabteilungsleiter:in. Je nach Situation sind aber auch z.B. Promovierende oder Leiter:innen von Studienprojekten angesprochen.

Rechtsgrundlage bestimmen

Nach unseren Datenschutzgesetzen ist jede Verarbeitung personenbezogener Daten verboten, sofern nicht entweder die betroffene Person darin eingewilligt hat oder eine Rechtsvorschrift die Verarbeitung gestattet. Gibt es weder eine Einwilligung noch eine Vorschrift als Erlaubnis, ist die Verarbeitung rechtswidrig.

Datenschutz-Grundsätze erfüllen

Die Datenschutzgrundverordnung (DSGVO) nennt Anforderungen, die jede Verarbeitung personenbezogener Daten zwingend erfüllen muss. Im Einzelnen werden als Stichpunkte genannt: „Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz“, „Zweckbindung“, „Datenminimierung“, „Richtigkeit“, „Speicherbegrenzung“ sowie „Integrität und Vertraulichkeit“. Jede verantwortliche Stelle muss zudem nachweisen können, dass ihre Verarbeitung diese Anforderungen erfüllt (Stichwort „Rechenschaftspflicht“).

Sicherheitsmaßnahmen (TOM) vorsehen

Um etwa die Anforderung „Integrität und Vertraulichkeit“ für die Datenverarbeitung zu erfüllen, können Methoden zur technischen Absicherung eingesetzt werden. Doch Technik kann nicht alles. Sicherheit hängt vor allem auch vom korrekten Verhalten aller Verarbeitungsbeteiligten ab. Die „Technisch-Organisatorischen-Maßnahmen (TOM)“ beschreiben, was Menschen und Maschinen tun, bzw. tun sollen, damit die Daten in den richtigen Händen bleiben.

VVT Eintrag erstellen

Für jede Verarbeitung personenbezogener Daten, die der Zuständigkeit der UW/H gGmbH unterliegt, ist ein Eintrag in das zentrale „Verzeichnis von Verarbeitungstätigkeiten (VVT)“ der UW/H gesetzlich vorgeschrieben. Darin werden alle wesentlichen Eigenschaften der Verarbeitung kurz zusammengefasst, um sie im Prüfungsfall unserer Aufsichtsbehörde (LDI.NRW) als erste Orientierung übergeben zu können. Auf Wunsch des Kanzlers wird das VVT beim betrieblichen Datenschutzbeauftragten (bDSB) geführt. Bitte sorgen Sie für einen korrekten VVT-Eintrag Ihrer Verarbeitung. Leitfragen zum konkreten Inhalt können Ihnen vom bDSB bereitgestellt werden.

AV/GV Verträge archivieren

Oft findet eine Datenverarbeitung allein durch die verantwortliche Stelle statt. Manchmal werden aber auch externe Dienstleister mit einbezogen (weisungsgebundene Auftragsverarbeiter). Für den Einbezug solcher Dienstleister ist ein Auftragsverarbeitungsvertrag (AV-Vertrag) gesetzlich vorgeschrieben. Ist ein externer Partner dagegen nicht weisungsgebunden, sondern bestimmt die

Zwecke und Mittel der Verarbeitung gleichberechtigt mit, handeln die Partner als „Gemeinsam Verantwortliche“. In diesem Fall ist in einer Vereinbarung festzulegen, welcher Partner welche Verpflichtungen aus der DSGVO erfüllt (GV-Vertrag).

Risikoanalyse/DSFA belegen

Verarbeitungen, die für die betroffenen Personen voraussichtlich ein hohes Risiko für ihre Rechte und Freiheiten zur Folge haben, erfordern dem hohen Risiko angepasste TOM zur Gewährleistung der Datensicherheit. Die Anpassung der TOM an das hohe Risiko und eine Abschätzung ihrer Wirksamkeit, geschieht im Rahmen der für solche Fälle vorgeschriebenen „Datenschutz-Folgenabschätzung (DSFA)“. Zur Entscheidung, ob eine DSFA erforderlich ist, werden die Verarbeitungs-Eigenschaften beim Eintrag in das VVT standardmäßig einer Risikoanalyse (Schwellenwertanalyse) unterzogen.

Datenschutzinfos vorab bereitstellen

Alle Personen, deren Daten in eine Verarbeitung eingehen, müssen im Voraus von der verantwortlichen Stelle über die Verarbeitung informiert werden. Das gilt unabhängig davon, ob die Verarbeitung auf Basis der Einwilligung oder einer anderen Rechtsgrundlage geschieht und grundsätzlich auch dann, wenn die Daten gar nicht bei der Person selbst erhoben werden. Der Umfang der Information ist in der DSGVO vorgeschrieben und deckt sich weitgehend mit den für das VVT zu dokumentierenden Eigenschaften. Muster-Informationen können vom bDSB bereitgestellt werden.

Auskunft (und andere Rechte) ermöglichen

Alle Personen, deren Daten verarbeitet werden, haben einen Anspruch auf Auskunft, Berichtigung, Löschung, Einschränkung der Verarbeitung, Widerspruch und Datenübertragbarkeit. Dazu kommt das Recht, eine einmal gegebene Einwilligung jederzeit auch widerrufen zu können. Jede Verarbeitung muss daher strukturell so aufgebaut werden, dass diese Rechte auch auf Dauer wirksam umgesetzt werden können. Dazu gehört die Benennung eindeutiger Ansprechpartner:innen für die betroffenen Personen und – insbesondere bei Verarbeitungen mit mehreren Partnern – eindeutige interne Regelungen zur Rechtebearbeitung, damit z.B. ein Löschwunsch auch in allen Teilverarbeitungen zuverlässig berücksichtigt werden kann.

Datenpannen mitteilen

Sollte es bei der Verarbeitung etwa zu einer unrechtmäßigen Offenbarung (Verlust der Vertraulichkeit), zur Verfälschung (Verlust der Datenintegrität) oder zur unbeabsichtigten Löschung (Verlust der Verfügbarkeit) von Daten kommen, muss diese „Datenpanne“ der Aufsichtsbehörde binnen 72 Stunden gemeldet werden. In besonders schweren Fällen auch den betroffenen Personen direkt. Das ist abhängig davon, wie stark sich die „Datenpanne“ auf die Betroffenen auswirkt. Sollte bei Ihrer Verarbeitung eine solche „Datenpanne“ geschehen, wenden Sie sich bitte umgehend an den betrieblichen Datenschutzbeauftragten.

Martin Rützler, bDSB der UW/H (GDDcert.)