Umsetzung der DSGVO in der Praxis

Fragen, Antworten, Muster

Bearbeitet von
Von: Lukas Feiler, und Bernhard Horn

1. Auflage 2018. Buch. 223 S. Kartoniert
ISBN 978 3 7046 7859 1
Format (B x L): 15.4 x 23.8 cm
Gewicht: 359 g

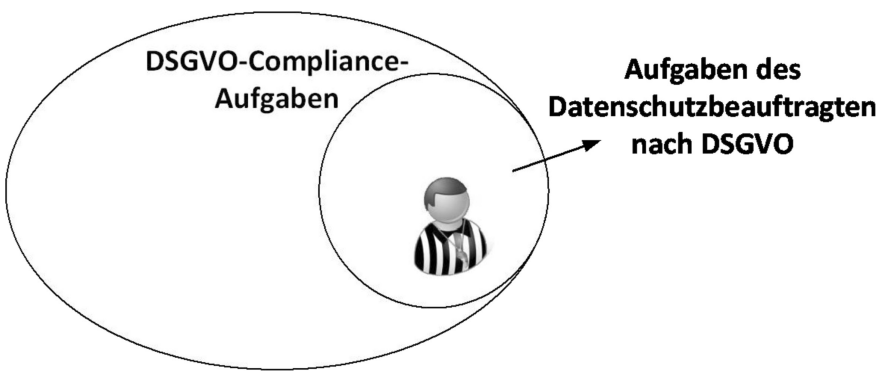
bußen hinzuweisen, für die das Management in vielen Fällen **persönlich haften** würde (siehe Fragen 95 und 97). Weiters empfiehlt es sich, an das Management bereits mit einem Umsetzungsplan entsprechend den folgenden elf Schritten heranzutreten, um nicht nur eine Herausforderung (DSGVO-Compliance), sondern auch gleich eine Lösung hierfür präsentieren zu können.

2 Schritt 2: Datenschutzbeauftragten bzw -manager ernennen und Zuständigkeiten klären

Die DSGVO verpflichtet Behörden und öffentliche Stellen (siehe hierzu Frage 2) sowie Unternehmen in den unten beschriebenen Fällen, einen sog Datenschutzbeauftragten zu bestellen. Nach dem Konzept der DSGVO hat der Datenschutzbeauftragte sehr beschränkte Aufgaben im Bereich der Datenschutz-Compliance. Er ist daher nicht umfassend dafür zuständig, die DSGVO im Unternehmen umzusetzen.

Insbesondere ist der Datenschutzbeauftragte nach der DSGVO nicht dazu verpflichtet, das Verzeichnis der Verarbeitungstätigkeiten zu führen (siehe Schritt 7) oder Datenschutz-Folgenabschätzungen durchzuführen (siehe Schritt 9).

Die Kernaufgaben eines Datenschutzbeauftragten bestehen vielmehr darin, die Organisation zu ihren Pflichten nach der DSGVO zu **beraten**, die Einhaltung dieser Pflichten zu **überwachen**, mit der Datenschutzbehörde **zusammenzuarbeiten** und als Anlaufstelle für Betroffene zu fungieren (vgl Art 38 f DSGVO). Das nach der DSGVO vorgesehene Aufgabengebiet des Datenschutzbeauftragten deckt daher nur einen kleinen Teil der nach der DSGVO verpflichtenden Compliance-Aufgaben ab (siehe Abbildung):



Aufgaben des Datenschutzbeauftragten

Um in Organisationen, in denen ein Datenschutzbeauftragter zu bestellen ist (oder freiwillig bestellt wird), alle DSGVO-Compliance-Aufgaben erfüllen zu können, ist es daher notwendig, entweder (1) zusätzlich zum Datenschutzbeauftragten einen organisationsinternen „Datenschutzmanager" zu bestellen oder (2) dem Datenschutzbeauftragten auch die Funktionen eines Datenschutzmanagers zu übertragen. Muss hingegen in einem Unternehmen kein Datenschutzbeauftragter bestellt werden, so können sämtliche Aufgaben – einschließlich jenen, welche die DSGVO für den Datenschutzbeauftragten vorgesehen hat – von einem Datenschutzmanager wahrgenommen werden. Die Aufgaben eines Datenschutzmanagers können freilich auch einer ganzen Abteilung übertragen werden.

Aufbauend auf die grundlegende Entscheidung, ob ein Datenschutzbeauftragter und/oder ein Datenschutzmanager bestellt wird, sollten folgende Entscheidungen getroffen werden:

- Welche **Befugnisse** soll der Datenschutzbeauftragte bzw -manager haben?
- Welche **sachliche Zuständigkeit** soll der Datenschutzbeauftragte bzw -manager haben? Ist er zB für alle Geschäftsbereiche zuständig?
- Welche **örtliche Zuständigkeit** soll der Datenschutzbeauftragte bzw -manager haben? Soll er zB auch ausländische Tochtergesellschaften betreuen?
- Wie soll der Datenschutzbeauftragte bzw -manager in die **Organisationsstruktur** eingebunden werden?
- Welche finanziellen und personellen **Ressourcen** sollen dem Datenschutzbeauftragten bzw -manager zugewiesen werden?

Bei der Beantwortung dieser Fragen ist zu berücksichtigen, dass die DSGVO für die Stellung des Datenschutzbeauftragten folgenden Rahmen zwingend vorgibt (Art 38 DSGVO):

- er ist **weisungsfrei**;
- er darf wegen der Erfüllung seiner Aufgaben nach der DSGVO nicht abberufen oder benachteiligt werden, genießt daher insbesondere **Kündigungsschutz**;
- er **berichtet unmittelbar der Geschäftsleitung**;
- er muss frühzeitig bei allen Datenschutzfragen **eingebunden** werden;
- das Unternehmen hat ihm **alle notwendigen Ressourcen** zur Verfügung zu stellen;
- ihm ist **Zugang zu allen IT-Systemen** zu gewähren, mit denen personenbezogene Daten verarbeitet werden;

B. Das Verzeichnis der Verarbeitungstätigkeiten

14. Ein Unternehmen hat weniger als 250 Mitarbeiter – Muss trotzdem ein Verzeichnis der Verarbeitungstätigkeiten geführt werden?

Ja – außer es handelt sich um einen Einzelunternehmer, der für seine Arbeit weder einen Computer verwendet, noch eine Kunden- oder Lieferantenkartei führt.

Die DSGVO sieht zwar eine **Ausnahme von der Pflicht zur Führung eines Verzeichnisses der Verarbeitungstätigkeiten** für Unternehmen mit **weniger als 250 Mitarbeitern** vor (Art 30 Abs 5 DSGVO). Diese Ausnahme ist allerdings nur dann anwendbar, wenn folgende Voraussetzungen erfüllt sind:

- die Datenverarbeitungen des Unternehmens bergen **keine Risiken für Betroffene** – dh es werden im Wesentlichen nur Daten verarbeitet, die öffentlich verfügbar sind (zB Name, Adresse, Telefonnummer);
- eine Verarbeitung personenbezogener Daten erfolgt **nur gelegentlich** (zB nur einmal in der Woche oder nur anlässlich der Ausstellung einer Rechnung mittels Registrierkassa) und
- die Verarbeitung umfasst **keine sensiblen Daten oder strafrechtlich relevanten Daten** (eine reguläre Lohnverrechnung, in der Krankheitstage oder Gewerkschaftszugehörigkeit erfasst sind, scheidet daher aus).

Bereits ein freiberuflicher Computergrafiker oder Programmierer hätte Schwierigkeiten, die oben genannten Voraussetzungen zu erfüllen, da die Kompromittierung des mit den Kunden geführten E-Mail-Verkehrs sehr wohl ein Risiko für die Betroffenen (Kunden) darstellen könnte und außerdem fraglich wäre, ob die regelmäßige E-Mail-Kommunikation mit Kunden noch die Voraussetzung der bloß „gelegentlichen" Verarbeitung personenbezogener Daten erfüllt.

Zudem sind auch manuelle Dateisysteme (papierbasierte Datenverarbeitungen) von den Regelungen der DSGVO umfasst, wenn die personenbezogenen Daten einzelner Betroffener nach einem Suchkriterium zugänglich sind.

Das trifft bei allen Kunden- oder Lieferantenkarteien oder sortierten Aktenordnern zu. Dass ein Unternehmen keine Liste mit (zumindest bestimmten umsatzstarken) Kunden führt, ist in der Praxis sehr selten.

Im Ergebnis werden daher nur Einzelunternehmer, die keinen Computer für ihre Arbeit verwenden und keine Kunden- oder Lieferantenkartei führen (zB ein Tischler oder Schuster), von der Führung eines Verzeichnisses der Verarbeitungstätigkeiten befreit sein.

15. Was muss im Verzeichnis der Verarbeitungstätigkeiten jedenfalls dokumentiert werden?

Die DSGVO enthält eine Liste von Angaben, die im Verzeichnis der Verarbeitungstätigkeiten **für jede Verarbeitungstätigkeit** (zB das Kundenbeziehungsmanagement oder die Personalverwaltung) dokumentiert werden müssen.

Hierbei verlangt die DSGVO für Verarbeitungstätigkeiten, bei denen die Organisation als Auftragsverarbeiter tätig ist (siehe hierzu Frage 16), wesentlich weniger Details, als bei Verarbeitungstätigkeiten, die die Organisation als Verantwortlicher durchführt.

Führt eine Organisation eine Verarbeitungstätigkeit als Verantwortlicher durch (zB die Personalverwaltung der eigenen Mitarbeiter), ist **Folgendes zu dokumentieren** (Art 30 Abs 1 DSGVO):

- Name und Kontaktdaten des **Verantwortlichen**;
- Wenn die Organisation nicht alleine über Mittel und Zwecke der Datenverarbeitung entscheidet, sondern gemeinsam mit anderen Organisationen (sog gemeinsam Verantwortliche): Name und Kontaktdaten der weiteren **gemeinsam Verantwortlichen**;
- Wenn der Verantwortliche nicht in der EU niedergelassen ist: Name und Kontaktdaten des zwingend zu bestellenden **Vertreters** (vgl Art 27 DSGVO);
- Wenn ein Datenschutzbeauftragter bestellt ist: Name und Kontaktdaten des **Datenschutzbeauftragten**;
- **Zwecke der Verarbeitung**: Die Zwecke jeder Verarbeitungstätigkeit werden ausschließlich vom Verantwortlichen festgelegt. Die Zweckbeschreibung muss dabei so gewählt werden, dass sich ein unbeteiligter Dritter leicht ein Bild machen kann, wofür Daten über die betroffenen Personen verarbeitet werden;
- Beschreibung der **Kategorien betroffener Personen** (zB Angestellte oder Kunden);

- Beschreibung der **Kategorien personenbezogener Daten**: eine abstrakte Beschreibung der einzelnen Datenkategorien (zB Name, Adresse, Geburtsdatum);
- Beschreibung der **Kategorien von Empfängern**, gegenüber denen die personenbezogenen Daten offengelegt werden: Im Verzeichnis müssen nicht notwendigerweise individuell benannte Empfänger angegeben werden, eine bloß generische Beschreibung der Empfängerkreise ist ausreichend (zB „alle Konzerngesellschaften"). Empfänger sind nicht nur andere Verantwortliche, gegenüber denen Daten offengelegt werden, sondern auch Auftragsverarbeiter (zB „IT-Dienstleister");
- Wenn Übermittlungen von personenbezogenen Daten an Empfänger in **Drittländern** außerhalb des EWR oder an internationale Organisationen stattfinden: die Namen der betreffenden Drittländer oder internationalen Organisation;
- **Aufbewahrungsfristen** der verschiedenen Datenkategorien: wie lange die Daten der einzelnen Datenkategorien aufbewahrt werden, bis sie gelöscht werden; ist eine exakte Angabe (zB „drei Jahre ab Beendigung des Vertragsverhältnisses") nicht möglich, können auch die Kriterien für die Festlegung der Aufbewahrungsdauer genannt werden (zB „bis zum Ablauf der gesetzlichen Aufbewahrungspflichten");
- Allgemeine Beschreibung der implementierten technischen und organisatorischen **Datensicherheitsmaßnahmen** (wenn möglich): Dafür empfiehlt sich die (einmalige) Ablage der Richtlinie zur Informationssicherheit (vgl Schritt 10 des Umsetzungsplans) im Verzeichnis der Verarbeitungstätigkeiten. Nur wenn für bestimmte Verarbeitungstätigkeiten spezielle Datensicherheitsmaßnahmen implementiert wurden, sollten diese individuell dokumentiert werden.

Die meisten dieser Informationen müssen in der Datenschutzmitteilung auch gegenüber den Betroffenen offengelegt werden (siehe Schritt 8, Zwischenschritt D des Umsetzungsplans).

Untenstehend ist ein **Muster** eines minimalistisch gestalteten Verzeichnisses der Verarbeitungstätigkeiten abgedruckt:

- In Abschnitt 1 sind allgemeine Informationen über die Organisation einzutragen.
- Die Tabelle in Abschnitt 2 ist für jede Verarbeitungstätigkeit zu reproduzieren, die die Organisation als Verantwortlicher ausübt.
- Die Tabelle in Abschnitt 3 ist für jede Verarbeitungstätigkeit zu reproduzieren, die die Organisation als Auftragsverarbeiter ausübt.

Muster eines minimalistischen Verzeichnisses der Verarbeitungstätigkeiten

Verzeichnis von Verarbeitungstätigkeiten

Inhalt

I. Allgemeine Information zur Organisation
II. Verarbeitungstätigkeiten, für welche die Organisation Verantwortlicher ist
III. Verarbeitungstätigkeiten, für welche die Organisation Auftragsverarbeiter ist

I. Allgemeine Information zur Organisation

1. Name und Kontaktdaten der Organisation	
Name/Firmenwortlaut der Organisation:	
Adresse:	
E-Mail-Adresse:	
2. Name und Kontaktdaten des Datenschutzbeauftragten (sofern bestellt)	
Name:	
Adresse:	
E-Mail-Adresse:	
Telefonnummer:	

II. Verarbeitungstätigkeiten, für welche die Organisation Verantwortlicher ist

[Nachfolgende Tabelle ist für jede Verarbeitungstätigkeit zu reproduzieren]

1. Allgemeine Angaben zur Verarbeitungstätigkeit		
LfNr:	*zB 1*	
Name der Verarbeitungstätigkeit:	*zB Kundenbeziehungsmanagement*	
2. Allfällige gemeinsam Verantwortliche		
Firmenwortlaut	Adresse	E-Mail-Adresse
…	…	…

3. Verarbeitungszwecke		
Liste der Verarbeitungszwecke, zB Erfüllung eines mit dem Kunden geschlossenen Vertrages.		
4. Kategorien Betroffener		
Liste der Kategorien betroffener Personen, zB Arbeitnehmer, Kunden.		
5. Datenkategorien		
Datenkategorie	Speicherdauer	
zB Name	*zB bis drei Jahre nach Vertragsbeendigung*	
…	…	
6. Kategorien von Empfängern (Verantwortliche und Auftragsverarbeiter)		
Kategorie von Empfängern	Typ (Verantwortlicher oder Auftragsverarbeiter)	Land (sofern außerhalb des EWR)
zB IT-Dienstleister	*zB Auftragsverarbeiter*	*zB EWR*
zB Konzerngesellschaften	*zB Verantwortlicher*	*zB EWR, USA, Kanada*
…	…	…
7. Beschreibung der technischen und organisatorischen Sicherheitsmaßnahmen		
…		

III. Verarbeitungstätigkeiten, für welche die Organisation Auftragsverarbeiter ist

[Nachfolgende Tabelle ist für jede Verarbeitungstätigkeit zu reproduzieren]

1. Allgemeine Angaben zur Verarbeitungstätigkeit	
LfNr:	*zB 1*
Name der Verarbeitungstätigkeit:	*zB Hosting von Websites*

2. Verantwortliche, in deren Auftrag diese Verarbeitungstätigkeit durchgeführt wird				
Firmenwortlaut	Adresse	E-Mail-Adresse	Kontaktdaten des Datenschutzbeauftragten*	Kontaktdaten des Vertreters**
…	…	…	…	…
* Sofern der jeweilige Verantwortliche einen Datenschutzbeauftragten bestellt hat: Name, Adresse, E-Mail-Adresse und Telefonnummer ** Sofern der jeweilige Verantwortliche nicht im EWR niedergelassen ist und einen inländischen Vertreter bestellt hat: Name, Adresse und E-Mail-Adresse				
3. Datenübermittlungen an Sub-Auftragsverarbeiter				
Firmenwortlaut	Adresse	E-Mail-Adresse	Kontaktdaten des Datenschutzbeauftragten*	Kontaktdaten des Vertreters**
…	…	…	…	…
* Sofern der jeweilige Sub-Auftragsverarbeiter einen Datenschutzbeauftragten bestellt hat: Name, Adresse, E-Mail-Adresse und Telefonnummer ** Sofern der jeweilige Sub-Auftragsverarbeiter nicht im EWR niedergelassen ist und einen inländischen Vertreter bestellt hat: Name, Adresse und E-Mail-Adresse				
4. Beschreibung der technischen und organisatorischen Sicherheitsmaßnahmen				
…				

Der Vollständigkeit halber ist darauf hinzuweisen, dass das oben abgedruckte Muster **zwei Konstellationen** nicht erfasst, die freilich für die allermeisten österreichischen Organisationen ohnedies nicht relevant sind:

- Sollte die **Organisation nicht in der EU niedergelassen** sein, müsste sie einen inländischen Vertreter bestellen (Art 27 DSGVO) und dessen Kontaktdaten ebenso im Verzeichnis der Verarbeitungstätigkeiten dokumentieren. Dies sieht das Muster nicht vor.
- Höchst seltene und im Übrigen gegenüber der Datenschutzbehörde **meldepflichtige Datenübermittlungen** in Drittländer wären ebenso im Verzeichnis der Verarbeitungstätigkeiten zu dokumentieren. Dies betrifft allerdings nur Übermittlungen, die (i) nicht wiederholt erfolgen, (ii) nur eine begrenzte Zahl von Personen betreffen, (iii) von zwingenden berechtigten Interessen des Verantwortlichen gedeckt sind und (iv)