2/2021
25 – 48

Judikatur
Strafhöhe
Viktoria Haidinger/Ernst M. Weiss

DATENSCHUTZ KONKRET

Recht | Projekte | Lösungen

Chefredaktion: Rainer Knyrim

Verwaltungsstrafverfahren

Praxis der DSB im Verwaltungsstrafverfahren

Herwig Zaczek und Ali Zanjani

Checkliste: Vorbereitung und Verhalten bei einer Datenschutzüberprüfung

Markus Oman, Siegfried Gruber und Viktoria Haidinger

Arbeit der VwG in der Pandemie

Interview mit Gregor Heißl, LVwG Tirol

WhatsApp im Unternehmen (II)

Stefanie Fasching

Einbindung des Betriebsrats in Datenschutz-Folgenabschätzung

Johannes Warter

Entwicklungen zum immateriellen Schadenersatz bei DSGVO-Verletzung

Andreas Rohner

BVwG: Informationspflicht und Rechtmäßigkeit

Martin Baumann und Marco Blocher

ISSN 2313-5409

dako.manz.at

MANZ

Österreichische Post AG PZ 18Z041356 P Verlag Manz, Gutheil Schoder Gasse 17, 1230 Wien

Markus Oman/Siegfried Gruber/Viktoria Haidinger
Geschäftsführender Gesellschafter O.P.P. – Beratungsgruppe/Prokurist O.P.P. – Beratungsgruppe/Wirtschaftskammer Österreich

Checkliste

Vorbereitung und Verhalten bei einer Datenschutzüberprüfung

Vorgehen der DSB, mögliche Fragen und Ablauf.

Diese Checkliste dient zur Vorbereitung auf eine Datenschutzüberprüfung gem Art 58 Abs 1 lit b DSGVO iVm § 22 Abs 1 DSG und beschreibt das Vorgehen der DSB, die möglichen Fragen der DSB und den möglichen Ablauf einer derartigen Überprüfung basierend auf Erfahrungen aus konkreten Verfahren.

Die DSB leitet eine Datenschutzüberprüfung mittels Schreiben an den Verantwortlichen oder Auftragsverarbeiter (AV) ein. Dieses hat folgenden Inhalt:

- Information über den Anlass der Datenschutzüberprüfung (Bezug zu einem konkreten Beschwerdeverfahren oder amtswegiges Verfahren);
- Übermittlung eines Fragenkatalogs bzw Aufforderung zur Übermittlung von Dokumenten;
- Festlegung einer Frist zur Beantwortung der Fragen bzw Übermittlung von Dokumenten (zumeist zwei bis vier Wochen);
- Information darüber, ob und wann eine Einschau geplant ist.

Welche Dokumente sind zu übermitteln?

In Verfahren nach dem DSG 2000 forderte die DSB konkrete Informationen zu den durchgeführten Verarbeitungen sowie den ergriffenen Datensicherheitsmaßnahmen an. Umgelegt auf die DSGVO ist daher davon auszugehen, dass die DSB folgende Unterlagen anfordert:

- Verarbeitungsverzeichnis (Art 30 Abs 1 oder Abs 2 DSGVO);
- Beschreibung der Datensicherheitsmaßnahmen iSd Art 32 DSGVO;
- Dokumentation der DSFA-Schwellenwertanalyse (Art 35 Abs 1 und 3 – 5 DSGVO) bzw der durchgeführten DSFA (Art 35 Abs 7 DSGVO);
- Auftragsverarbeiterverträge iSd Art 28 DSGVO;
- Betriebsvereinbarungen, sofern datenschutzrechtlich relevant;
- Datenschutzerklärungen nach Art 13, 14 DSGVO.

Mögliche Fragen der DSB

Die Fragen beziehen sich auf die konkrete Verwendung von Daten natürlicher Personen (va Kunden, Interessenten, Lieferanten, Patienten, aber auch Mitarbeiter) im Rahmen der Tätigkeit des Verantwortlichen bzw AV. Sollte die DSB nach Erhalt der Antworten noch weitere Informationen benötigen, ist es möglich, dass eine Aufforderung zur Beantwortung ergänzender Fragen an den Verantwortlichen bzw AV gestellt wird. Auch in diesen Fällen wird in der Regel eine Frist zur Beantwortung von zwei bis vier Wochen eingeräumt.

Praxistipp:

Je nach Anlassfall der Datenschutzüberprüfung bzw Art der Verarbeitung bzw Branchenzugehörigkeit des Verantwortlichen kann der Inhalt der Fragen variieren. Einzelne, über den übermittelten Fragekatalog hinausgehende Fragen können auch mündlich im Rahmen der Einschau gestellt werden.

Organisation und Arbeitsweise

- 1a) Stellen Sie bitte kurz Ihre Einrichtung/Trägergesellschaft vor (bspw durch Organigramm) und geben Sie bekannt, welche Mitarbeiter bzw Organisationseinheit sich über die in Ihrer Einrichtung verarbeiteten Daten informieren dürfen.
- 1b) Betreiben Sie Datenbanken (bspw für CRM, Kunden-Datenbanken, Vertriebsakten, Krankenakten, Personaldaten) und wenn ja, wer hat darauf Zugriff? Wenn Außenstehende (fremde Personen) Zugriff haben, wie ist der Zugriff geregelt bzw ist der Zugriff auf bestimmte Personen- oder Berufsgruppen eingeschränkt? Wie erfolgt der Zugriff (bspw über eine Internetverbindung)?
- 1c) Werden die Akten/Unterlagen/Personaldaten voll, nur teilweise oder gar nicht automationsunterstützt verarbeitet (bspw in Papierakten)?

Rolle und Einhaltung datenschutzrechtlicher Grundsätze (Art 5 DSGVO)

- 2a) Wie definieren Sie Ihre datenschutzrechtliche Rolle? Sehen Sie sich als Verantwortlicher oder als AV? Falls Sie sich als AV sehen, geben Sie jene Verantwortlichen an, die Ihre Einrichtung regelmäßig als datenschutzrechtlicher AV in Anspruch nehmen.
- 2b) Art 5 Abs 1 lit b DSGVO bestimmt, dass personenbezogene Daten nur für festgelegte, eindeutige und rechtmäßige Zwecke ermittelt und nicht in einer mit diesen Zwecken unvereinbaren Weise weiterverwendet werden dürfen.
  - Für welche konkreten und rechtmäßigen Zwecke ermittelt und verwendet Ihre Einrichtung personenbezogene Daten?
  - Wie stellen Sie die Einhaltung dieses Grundsatzes sicher?
- 2c) Art 5 Abs 1 lit c DSGVO bestimmt, dass Daten nur, soweit sie für den Zweck der Datenanwendung wesentlich sind, verwendet werden und ihre Verwendung über diesen Zweck nicht hinausgehen darf.
  - i) Wie stellen Sie die Einhaltung dieses Grundsatzes sicher?
  - ii) Welche Daten werden von Ihnen regelmäßig erhoben?

- 2 d) Art 5 Abs 1 lit d DSGVO bestimmt des Weiteren, dass Daten nur so verwendet werden dürfen, dass sie im Hinblick auf den Verwendungszweck im Ergebnis sachlich richtig und, wenn nötig, auf den neuesten Stand gebracht sind.
  - Wie stellen Sie die Einhaltung dieses Grundsatzes sicher?
- 2 e) Art 5 Abs 1 lit e DSGVO bestimmt, dass Daten nur so lange in personenbezogener Form aufbewahrt werden dürfen, als dies für die Erreichung der Zwecke, für die sie ermittelt wurden, erforderlich ist.
  - Wie stellen Sie die Einhaltung dieses Grundsatzes sicher?
  - Wie lange bewahren Sie Daten in personenbezogener Form auf?
  - Auf welche (konkrete) Rechtsgrundlage können Sie sich dabei stützen?
- 2 f) Laut Art 5 Abs 1 lit e DSGVO haben Sie für den technisch-organisatorischen Datenschutz zu sorgen.
  - Wie stellen Sie die Einhaltung dieses Grundsatzes sicher?
- 2 g) Als Verantwortlicher unterliegen Sie der Rechenschaftspflicht iSd Art 5 Abs 2 DSGVO.
  - Wie stellen Sie die Einhaltung dieses Grundsatzes sicher?

Rechtsgrundlagen der Verarbeitungen (Art 6 DSGVO)

- 3 a) Verarbeiten Sie personenbezogene Daten auf Grundlage einer Einwilligung betroffener Personen (Art 6 Abs 1 lit a oder Art 9 Abs 2 lit a DSGVO)?
  - Wenn ja, wie erbringen Sie den Nachweis des Vorliegens der Einwilligung (Art 7 Abs 1 DSGVO)?
- 3 b) Verarbeiten Sie personenbezogene Daten auf Basis „berechtigter Interessen" gem Art 6 Abs 1 lit f DSGVO?
  - Wenn ja, begründen Sie das Vorliegen dieser berechtigten Interessen?
- Findet eine Weiterverwendung personenbezogener Daten auch für andere Zwecke statt als jene, für die diese Daten ursprünglich erhoben wurden?
  - Wenn ja, welche derartige Weiterverwendung findet statt? Begründen Sie die Rechtmäßigkeit dieser Weiterverwendung.

Datenübermittlungen (Art 6 DSGVO)

- 4 a) Wenn Sie Daten an Dritte übermitteln (dh, nicht an AV), prüfen Sie deren ausreichende gesetzliche Zuständigkeit oder rechtliche Befugnis[1] und ob durch den Zweck und Inhalt der Übermittlung die Interessen des Betroffenen nicht überwiegen?
  - i) An welche Empfänger im Inland und in der Union werden durch Sie Daten regelmäßig übermittelt? Woraus ergibt sich deren ausreichende gesetzliche Zuständigkeit oder rechtliche Befugnis?
  - ii) Auf welche Rechtsgrundlage (bspw Einwilligung) können Sie sich dabei stützen?
- 4 b) Art 28 DSGVO regelt die Zulässigkeit der Überlassung von Daten zur Erbringung von Datenverarbeitungen im Auftrag und die Plichten des AV.
  - i) Ziehen Sie zur Erfüllung Ihrer Aufgaben AV heran (bspw zur technischen Wartung)?
  - ii) Falls ja, wie stellen Sie die Einhaltung der Plichten eines Dienstleisters sicher?
- 4 c) Übermittlung und Überlassung von Daten in das Ausland.
  - i) Übermitteln Sie Daten an Empfänger/AV in EWR-Staaten?
  - ii) Übermitteln Sie Daten an Empfänger/AV außerhalb des EWR? Falls ja, auf welche Rechtsgrundlage bzw auf welchen Ausnahmetatbestand können Sie sich dabei stützen? Wie stellen Sie das Vorliegen eines angemessenen Datenschutzes bei Empfängern außerhalb des EWR sicher? Legen Sie bspw dem Empfänger Verwendungsbeschränkungen auf?
  - iii) Bewahren Sie eine nachvollziehbare Dokumentation aller Auslandsübermittlungen auf?
  - iv) Wie gehen Sie vor, wenn Sie feststellen, dass bereits übermittelte Daten zu berichtigen oder zu löschen sind?
  - v) Speichen Sie personenbezogene Daten nur in Österreich oder auch im Ausland? Nehmen Sie Cloud-Services für Ihre Aufgabenerfüllung in Anspruch?

Datensicherheitsmaßnahmen (Art 32 DSGVO) und Informationspflichten bei Verletzungen (Art 33 f DSGVO)

- 5 a) Welche Maßnahmen ergreifen Sie, um unberechtigte Zugriffe (auch durch nicht-autorisierte Mitarbeiter) auf personenbezogene Daten hintanzuhalten?
- 5 b) Gibt es Mitarbeiter, die Zugriff auf alle Daten haben? Gibt es Zugriffsbeschränkungen?
- 5 c) Zeichnen Sie – etwa mittels Zugriffsprotokollen – die einzelnen Zugriffe auf? Falls ja, wie lange bewahren Sie Protokolldaten auf?
- 5 d) Wie stellen Sie fest, dass unautorisiert auf Daten zugegriffen wurde (externer und/oder interner Zugriff)?
- 5 e) Wie ist der Zugang zu Krankengeschichten/Personaldaten geregelt (bspw Benutzername, Passwort)?
- 5 f) Wenn es zur Verletzung des Schutzes personenbezogener Daten kommt: Wie ist bei Ihnen der Prozess zur Prüfung der Verpflichtungen nach Art 33 (Meldung an die DSB) und Art 34 (Benachrichtigung Betroffener) geregelt?

Betroffenenrechte

- 6 a) Wie erfüllen Sie Ihre Informationspflichten nach Art 13, 14 DSGVO?
- 6 b) Gem Art 15 DSGVO hat jede natürliche Person das Recht auf Auskunft der zu seiner Person verarbeiteten Daten.
  - i) Wie gehen Sie im Falle einer zulässigen Anfrage vor?

[1] Zur Weitergeltung der Idee des § 7 Abs 1 DSG 2000 s *Haidinger* in *Knyrim*, Praxishandbuch[4] Rz 5.103.

- ii) Welche Auskünfte werden erteilt? Gehen Sie dabei über den von Art 15 DSGVO gesteckten Rahmen hinaus?
- iii) Welche Auskünfte werden nicht erteilt?
- iv) Wie oft (Schätzung) sind Sie pro Jahr mit Auskunftsbegehren konfrontiert?

- 6 c) Nach der DSGVO hat jedermann das Recht auf Berichtigung (Art 16) oder Löschung (Art 17) der zu seiner Person verarbeiteten Daten.
  - i) Wann löschen Sie Daten selbständig?
  - ii) Wie gehen Sie im Fall eines zulässigen Antrags auf Berichtigung oder Löschung vor?
  - iii) Wie oft (Schatzung) sind Sie pro Jahr mit Anträgen auf Berichtigung oder Löschung konfrontiert?

Konkrete Datenanwendungen

- 7 a) Setzen Sie Videoüberwachungen ein? Falls ja, zu welchem Zweck? Wo sind die Kameras angebracht? Sind die Videoüberwachungen durch Hinweisschilder gekennzeichnet?
- 7 b) Werden medizinische Studien unter Rückgriff auf bestimmte Patienten durchgeführt? Wenn ja, wie gehen Sie dabei vor? Wird die Einwilligung der jeweiligen Patienten eingeholt?
- 7 c) Verwenden Sie automatisierte Recruiting-Tools und setzen Sie Assessment-Center ein? Werden dabei automatisierte Entscheidungen im Einzelfall gem Art 22 DSGVO getroffen?
- 7 d) Setzen Sie arbeitsmedizinische Verwaltungsprogramme ein? Welche Untersuchungen dokumentieren Sie darin (etwa Vorsorge-Untersuchungen, Titerstatus, andere gesetzlich vorgeschriebene und andere wiederkehrende Untersuchungen wie zB Strahlenschutz, Hepatitis, SARS-CoV-2)? Wer hat Zugriff auf dieses Programm?

Weitere Informationen

- Fragen von anderen Behörden: Bayerisches Landesamt für Datenschutzaufsicht www.lda.bayern.de/de/kontrollen.html
- Kriterienkatalog zur Querschnittsprüfung in der Wirtschaft 2018/19 des Landesbeauftragten für den Datenschutz Niedersachsen https://lfd.niedersachsen.de/startseite/datenschutzreform/ds_gvo/kriterien-querschnittspruefung-179455.html

Dako 2021/19