
TaylorWessing
DSGVO-konform oder nicht?
Audits als Mittel zur Selbstkontrolle

Der europäische Gesetzgeber setzt zur Gewährleistung eines hohen Datenschutzniveaus innerhalb der EU auf eine starke Eigenverantwortung datenverarbeitender Unternehmen. Gesetzlich trifft sie eine Rechenschaftspflicht. Das bedeutet, Unternehmen müssen nicht nur die Einhaltung der DSGVO sicherstellen, sondern ihre Rechtskonformität bei Aufforderung durch die Aufsichtsbehörden auch nachweisen können. Sowohl anlassbezogene als auch anlasslose Prüfungen durch die Aufsichtsbehörden sind denkbar.

Gelingt Unternehmen der Konformitäts-Nachweis nicht, drohen hohe Bußgelder. Rekordverdächtige Bußgeldsummen zeigen, dass die Aufsichtsbehörden diese Drohung auch wahrmachen. Mit einer einmaligen Anpassung der internen Prozesse an die gesetzlichen Vorgaben ist es aber nicht getan. Unternehmen müssen den geschaffenen Datenschutzstandard ständig aufrechterhalten. Das gilt umso mehr, als es sich bei der DSGVO nicht um einen bereits etablierten Rechtsrahmen handelt, sondern die Regelungen erheblich durch die Stellungnahmen der Aufsichtsbehörden sowie die Gerichte konkretisiert werden. Folglich hat sich die spezifische Auslegung als auch Priorisierung einzelner Verpflichtungen aus der DSGVO seit Inkrafttreten der Verordnung verändert – mit entsprechenden Handlungspflichten für die Unternehmen.

Unternehmen sollten daher sicherstellen, dass die geschaffenen Datenschutzstandards im Unternehmen auch tatsächlich gelebt und insbesondere auch bei neuen Projekten umgesetzt werden. Mehr als zwei Jahre nach Inkrafttreten der DSGVO ist es Zeit, die eigene Umsetzungsleistung kritisch zu überprüfen. Dazu bietet sich die Durchführung eines DSGVO-Audits an.

Sollte die DSGVO intern noch nicht umgesetzt worden sein, bietet sich eine schrittweise Implementierung der zahlreichen Datenschutz-Vorgaben an. Dabei kann Ihnen unser Leitfaden zur Implementierung der EU-Datenschutz-Grundverordnung als Hilfestellung dienen.

Vorteile eines DSGVO-Audits

Eine explizite gesetzliche Pflicht zur Durchführung von Audits kennt die DSGVO nicht. Lediglich im Hinblick auf technische und organisatorische Datenschutzmaßnahmen verpflichtet die DSGVO datenverarbeitende Unternehmen ausdrücklich zur Durchführung regelmäßiger Kontrollverfahren (z.B. Penetrationstests) in Abhängigkeit vom Datenverarbeitungsrisiko (Art. 32 Abs. 1 lit. d DSGVO).

Umfassende Audits zur Rechtskonformität können Unternehmen jedoch den Nachweis der Einhaltung der DSGVO erleichtern. Dadurch können sie ihrer gesetzlichen Rechenschaftspflicht gerecht werden.

- Zum einen wird mit dem Audit die interne Umsetzung der DSGVO bewertet und dies entsprechend dokumentiert. Dies kann im besten Fall zum Nachweis der DSGVO-Konformität gegenüber der Aufsichtsbehörde genutzt werden. Selbst wenn ein vollumfänglicher Nachweis über die Einhaltung der Vorgaben der DSGVO mit Hilfe des Audits nicht gelingen sollte, dokumentiert der Audit entsprechende Bemühungen und ist daher bei der Berechnung von Bußgeldern zugunsten des Unternehmens zu berücksichtigen

- Zum anderen kann ein Audit interne Fehler und Unzulänglichkeiten bei der DSGVO-Umsetzung aufdecken und dabei Unternehmen ihren Anpassungsbedarf für umfassende Rechtskonformität aufzeigen. Selbst zwei Jahre nach Inkrafttreten der DSGVO ist vielen Unternehmen eine vollständige Umsetzung noch nicht gelungen, was rekordverdächtige Bußgelder in der EU belegen

Daneben sind Audits ein „Realitätscheck". Viele Unternehmen waren bei der Umsetzung der Vorgaben der DSGVO unter Zeitdruck. Vielfach wurden daher zunächst Prozesse erarbeitet und Leitlinien erstellt. Die tatsächliche Umsetzung derselben in der alltäglichen Arbeit des Unternehmens war zumeist von untergeordneter Rolle. Häufig werden die geschaffenen Standards nicht gelebt oder intern nicht konsequent umgesetzt. Werden bspw. die internen IT-Systeme nicht entsprechend der Standards angepasst oder eingeführte Daten-Löschpflichten nicht umgesetzt, findet Rechtskonformität nur „auf dem Papier statt". Unternehmen riskieren, dass diese Defizite in der DSGVO-Umsetzung anlässlich von Datenschutzverletzungen, Auskunftsansprüchen Betroffener oder im Rahmen behördlicher Verfahren zu Tage treten. Dies sollten Unternehmen zur Vermeidung entsprechender Bußgeldrisiken in jedem Fall vermeiden. Mit einem Audit lässt sich überprüfen, ob die geschaffenen Maßnahmen erfolgreich waren und tatsächlich zu einem höheren Datenschutzniveau geführt haben. Audits sind damit ein wichtiges Mittel zur Selbstkontrolle. Diesem Aspekt sollte daher im Rahmen eines Audits besondere Beachtung zukommen.

Interner oder externer Audit?

Es ist grundsätzlich möglich, einen DSGVO-Audit intern oder extern durchzuführen. Entscheidend für die Wahl des richtigen Verfahrens ist, welches Ziel mit der Überprüfung verfolgt wird.

- Ein externer Audit wird von einer unabhängigen Stelle durchgeführt und bietet sich daher insbesondere zur Erlangung eines objektiven Nachweises über die eigene DSGVO-Konformität an

- Ein interner Audit ist dahingegen vor allem als Mittel der Selbstkontrolle geeignet, um die eigene Umsetzungsleistung zu überprüfen, einzelne Datenschutzlücken zu erkennen und gegebenenfalls zu beheben. Ein hinreichend unabhängiger und objektiver Nachweis über die interne Einhaltung der DSGVO-Vorgaben kann durch eigene Mitarbeiter u.U. schwieriger erbracht werden. Allerdings lässt sich mit einem internen Audit herausfinden, ob die ergriffenen Datenschutzmaßnahmen wirken

Ablauf eines DSGVO-Audits

Der grundlegende Ablauf eines DSGVO-Audits lässt sich wie folgt beschreiben:

1 Festlegung des Audit-Ziels

Als ersten Schritt sollten Unternehmen ihr Audit-Ziel festlegen. Soll eine vollumfängliche Überprüfung des DSGVO-Konformität stattfinden oder soll diese auf einzelne, kritische Unternehmensbereiche mit besonders hohem Datenschutzrisiko beschränkt werden? Soll anstelle einer umfänglichen Prüfung lediglich ein TOM-Audit zur Überprüfung der getroffenen Datenschutzmaßnahmen durchgeführt werden?

2 Auditplanung

Ist das Auditziel festgelegt, kann der Ablauf des Audits geplant werden. Ausgehend vom Auditziel lässt sich festlegen, ob es mit einem internen oder externen Audit bestmöglich erreicht werden kann. In Vorbereitung des Audits sollte zunächst ein Ablaufplan erstellt werden, der neben dem zeitlichen Rahmen auch die internen Verantwortlichkeiten für den DSGVO-Audit festlegt (z.B. wer ist Ansprechpartner für die externen Prüfer, wer ist intern für die Sammlung der Prüfdokumente zuständig).

Das Kernstück der Auditplanung bildet die Erstellung des Fragenkatalogs, anhand dessen der Audit durchgeführt wird. Dabei sollten v.a. Besonderheiten im Unternehmen nicht unberücksichtigt bleiben (z.B. Verarbeitung besonderer Datenkategorien im Unternehmen, Verarbeitung von Daten über Kinder). Für DSGVO-Audits werden regelmäßig Fragen zu den folgenden Datenschutzaspekten im Katalog abgebildet:

- Einzelheiten zum Unternehmen (z.B. Sektor, Unternehmensgegenstand, Organigramm, Mitarbeiter-anzahl)
- Abfrage der Datenschutzdokumentation (z.B. Datenschutzerklärung, Verzeichnis von Verarbeitungs-tätigkeiten, Einzelheiten zu genutzten Dienstleistern und Vorlage geschlossener Datenschutzverträge)
- Fragen zur Datenschutzorganisation (z.B. Vorhandensein eines Datenschutzbeauftragten, durchgeführte Datenschutzfolgenabschätzungen, Datenschutzkonzept, Zugriffsrechte auf Daten, Umgang mit Betroffenenrechten, Mitarbeiterschulungen)
- Informationen zu den eingesetzten IT-Systemen (z.B. Serverstandorte, durchgeführte Sicherheitsüberprüfungen, Zugriffsregelungen, Verschlüsselungsstandards)

Die Fragen sind grundsätzlich schriftlich und/oder durch Vorlage entsprechender Dokumente zu beantworten.

Bei der Planung sollten Unternehmen jedoch auch dafür sorgen, dass sie im Rahmen des Audits herausfinden können, ob die internen Datenschutzstandards tatsächlich gelebt werden. Dafür bieten sich zum einen (stichprobenartige) Mitarbeiterbefragungen an. Ein umfassenderes Bild kann jedoch eine faktische Untersuchung im Unternehmen liefern. Im Rahmen des Audits sollte z.B. überprüft werden, ob Mitarbeiter mit den internen Datenschutzvorgaben vertraut sind, ob die Datenschutzvorgaben vollständig umgesetzt werden und ob sie insb. bei neuen Projekten berücksichtigt werden. Im Rahmen einer faktischen Untersuchung könnten zu diesem Zweck etwa testweise Anfragen zur Ausübung von Betroffenenrechten gestellt werden oder ähnliche Datenschutzszenarien erprobt werden.

Ablauf eines DSGVO-Audits

3 Durchführung des Audits

Die Durchführung des Audits erfolgt durch die Überprüfung der beantworteten Fragen und vorgelegten Dokumente anhand der Vorgaben der DSGVO. Zur Überprüfung der internen Umsetzung der DSGVO-Pflichten findet darüber hinaus ggf. eine faktische Untersuchung im Unternehmen statt. Der Ist-Zustand der internen Datenschutzprozesse steht dabei auf dem Prüfstand.

4 Prüfbericht und Dokumentation

Die Ergebnisse des DSGVO-Audits werden in einem Prüfbericht zusammengefasst. Dieser dient zum einen der internen Dokumentation des durchgeführten Audits (Auditziel, Prüfgegenstand, Vorgehensweise, Übersicht der geprüften Dokumente, Prüfergebnis) und ermöglicht Unternehmen andererseits die Erfüllung ihrer Rechenschaftspflicht ggü. Aufsichtsbehörden.

5 Umsetzung der Audit-Empfehlungen

Wurde im Rahmen der Überprüfung eine Abweichung zwischen Ist- und Soll-Zustand im Hinblick auf die DSGVO-Konformität festgestellt, enthält der Prüfbericht Empfehlungen zu möglichen Maßnahmen, um diese Lücken zu beheben. So könnten ggf. Maßnahmen auf rechtlicher Ebene (z.B. Überarbeitung der Einwilligungserklärungen) oder auf technisch-organisatorischer Ebene erforderlich sein. Die Umsetzung der Empfehlungen obliegt dann dem geprüften Unternehmen, um DSGVO-Compliance zu erreichen.

Ausblick: Zertifizierungsverfahren

Ein externer DSGVO-Audit ließe sich auch mit dem Ziel durchführen, eine Zertifizierung gem. Art. 42 DSGVO zu erlangen. Nach dem Willen des Gesetzgebers können entsprechende Zertifikate rechtssicher zur Erfüllung der Rechenschaftspflicht gegenüber Aufsichtsbehörden vorgelegt werden oder ggf. Datentransfers in Drittländer absichern. Darüber hinaus könnten sie einen Vorteil gegenüber Wettbewerbern bieten, indem sie Unternehmen am Markt als besonders datenschutzkonform ausweisen.

Die Ausgestaltung entsprechender Zertifizierungsverfahren obliegt in erster Linie den Mitgliedstaaten und Datenschutzaufsichtsbehörden. Die Durchführung der Zertifizierungsverfahren samt Vergabe von Zertifikaten soll akkreditierten Zertifizierungsstellen obliegen. In der EU gibt es jedoch bisher keine akkreditierten Zertifizierungsstellen und daher auch keine entsprechenden Zertifikate.

Perspektivisch könnten derartige Verfahren allerdings den Nachweis der DSGVO-Compliance in Folge von Audits wesentlich erleichtern und würden daher einen zusätzlichen Compliance-Mehrwert bieten. Der genaue Ablauf derartiger Verfahren bleibt abzuwarten.

Ihre Ansprechpartner

Dr. Paul Voigt, Lic. en Derecho, CIPP/E

Tel +49 (0)30 88 56 36-408
p.voigt@taylorwessing.com

Anwalt des Jahres 2020 für Datenschutzrecht
Best Lawyers in Kooperation mit dem Handelsblatt

Ausgezeichnet als „Name der nächsten Generation" für Datenschutzrecht
Legal 500 Deutschland, 2020

Top-Anwalt für Datenschutzrecht in Deutschland
WirtschaftsWoche 2020

Wiebke Reuter

+49 30 885636-131
w.reuter@taylorwessing.com

Rita Danz

+49 30 885636-158
r.danz@taylorwessing.com

1000+ Anwälte
300+ Partner
28 Büros
16 Jurisdiktionen

Belgien	Brüssel
China	Peking* I Hongkong I Shanghai*
Deutschland	Berlin I Düsseldorf I Frankfurt I Hamburg I München
Frankreich	Paris
Großbritannien	Cambridge I Liverpool I London I London Tech City
Niederlande	Amsterdam I Eindhoven
Österreich	Wien I Klagenfurt*
Polen	Warschau
Slowakei	Bratislava
Südkorea	Seoul**
Tschechien	Prag I Brno*
Ukraine	Kiew
Ungarn	Budapest
USA	Silicon Valley* I New York*
VAE	Dubai

* Repräsentanzen ** Assoziierte Büros

Europe > Middle East > Asia

taylorwessing.com