Markus Näf
Master of Law, Rechtsanwalt
Lehrbeauftragter für Informatikrecht und Projektmanagement an der FHS St. Gallen
Partner
Telefon +41 58 258 10 00
markus.naef@bratschi.ch

Julian Powell
MLaw, LL.M.
Telefon +41 58 258 10 00
julian.powell@bratschi.ch

Jährlicher Datenschutzaudit im Unternehmen – Wunsch oder Pflicht?

Die seit dem 25. Mai 2018 geltende EU-Datenschutz-Grundverordnung (DSGVO) bringt für Schweizer Unternehmen mit EU-Beziehungen neue Pflichten. Die Pflicht unter dem unscheinbaren Begriff «Accountability» hat vermutlich die grössten Auswirkungen auf die Unternehmen. Diese müssen neu den Nachweis der Erfüllung der neuen Datenschutzvorschriften erbringen und deren Einhaltung auch periodisch überprüfen. Die Revision des schweizerischen Datenschutzgesetzes (DSG) wird eine analoge Vorschrift bringen.

1. Grundlagen in der DSGVO

Seit dem 25. Mai 2018 gilt in der EU die neue Datenschutz-Grundverordnung (DSGVO). Das neue Regelwerk trägt gewichtige Auswirkungen für Unternehmen weit über die Grenzen der EU hinaus mit sich. Insbesondere werden die Datenschutzgrundsätze gefestigt, die Rechte der betroffenen Personen ausgebaut und Sanktionen für Verstösse verschärft.

Zur Gewährleistung der Befolgung der neu eingeführten materiellen Pflichten, sieht die DSGVO auch zahlreiche formelle Pflichten vor, denen eine regelmässige Überprüfung der Einhaltung der datenschutzrechtlichen Vorgaben gemeinsam ist.

Neben dem Nachweis der Umsetzung von Einzelmassnahmen muss die Einhaltung der Datenschutzvorschriften regelmässig überprüft werden. Verstösse gegen die Datenschutzbestimmungen werden mit Bussen sanktioniert. Positiv formuliert heisst das *«eine erhöhte Selbstverantwortung des Unternehmens»*. Diese Verantwortung kann nur durch jährliche Überprüfungen der Einhaltung der formellen Vorschriften und der Wirksamkeit der Datenschutzmassnahmen wahrgenommen werden.

Aktuell sind diese Bestimmungen auch für Unternehmen in der Schweiz Pflicht, wenn die DSGVO aufgrund der Geschäftstätigkeit auf sie anwendbar ist. Die geplante Revision des schweizerischen Datenschutzgesetzes wird im Jahr 2020 voraussichtlich die gleichen Pflichten für alle Unternehmen in der Schweiz vorschreiben.

2. Die Pflicht zum Datenschutzaudit

Klare Vorgaben, wie die Nachweispflicht umzusetzen ist, macht die DSGVO nicht. Die Formulierung in Art. 24 DSGVO legt jedoch nahe, dass eine Art Datenschutz-Managementsystem (DSMS) zu implementieren ist, da festgelegt wird, dass die Massnahmen überprüft und aktualisiert werden müssen. Es genügt also nicht, Massnahmen einmalig festzulegen und zu implementieren, sondern die Wirksamkeit der ergriffenen Massnahmen ist regelmäßig zu überprüfen und gegebenenfalls sind Anpassungen vorzunehmen. Eine nachhaltige Überprüfung der vorgegebenen Pflichten dürfte vor allem für grössere Unternehmen nur über einen regelmässigen Datenschutzaudit zu bewältigen sein.

Die in Art. 5 Abs. 1 DSGVO verankerten Datenschutzgrundsätze (Rechtmässigkeit, Treu und Glauben, Transparenz, Zweckbindung, Datenminimierung, Richtigkeit, Integrität) sind allesamt von einer Rechenschaftspflicht (Art. 5 Abs. 2 DSGVO) begleitet. Unternehmen werden damit in die Pflicht genommen, den Nachweis der Einhaltung der Datenschutzvorschriften zu erbringen. Der Grundsatz der Rechenschaftspflicht (englisch auch *«Accountability»* genannt) durchzieht das gesamte DSGVO-Regelwerk. Zu diesem Zweck stellt die DSGVO verschiedene spezifische Dokumentationspflichten auf, namentlich die Führung sog. Verzeichnisse der Verarbeitungsaktivitäten (Art. 30 DSGVO), die Sicherstellung der Wirksamkeit von erteilten Einwilligungen (Art. 7 und 8 DSGVO) sowie hinsichtlich der Aufzeichnung von Datenschutzverletzungen (Art. 33 DSGVO).

Eine Pflicht zur Überprüfung der Auswirkungen der Datenbearbeitungsprozesse ergibt sich ebenfalls aus dem risikobasierten Ansatz der DSGVO, wonach technische und organisatorische Datenschutzmassnahmen anhand der Art, des Umfangs, der Umstände und Zwecke der Datenbearbeitung sowie der Eintrittswahrscheinlichkeit und der Schwere der Risiken für die Rechte und Freiheiten der betroffenen Personen umzusetzen sind (Art. 24 und 32 DSGVO). Der risikobasierte Ansatz wird auch bei der Prüfung der Erforderlichkeit der Bestellung eines Datenschutzbeauftragten gefordert (Art. 37 DSGVO) sowie der Durchführung einer Datenschutz-Folgeabschätzung (Art. 35 DSGVO).

Da sich Unternehmen und deren Datenbearbeitungsprozesse laufend entwickeln, verlangen die Rechenschaftspflicht und die Risikoüberprüfung eine regelmässige Nachführung des Audits. Eine taugliche Risikoüberprüfung wiederrum kann nur mit einem Datenschutzaudit erfolgreich umgesetzt werden. Wir erachten eine jährliche Durchführung des Audits für angemessen und zielführend, um Datenschutzverstösse zu vermeiden und angedrohten Sanktionen (bis zu EUR 20 Mio. oder 4% des globalen Jahresumsatzes) zu entgehen oder diese zumindest zu reduzieren.

Ein Audit kann intern oder extern erfolgen. Er ist jedoch nicht zu verwechseln mit einer Datenschutz-Zertifizierung nach der DSGVO oder dem DSG.

3. Datenschutz-Management-System (DSMS)

Die Massnahmen im Datenschutz können in einem DSMS zusammengefasst werden. Ein solches basiert auf den Standards ISO 27001 für *«IT-Sicherheitsverfahren – Informationssicherheits-Managementsysteme – Anforderungen»* und ISO 27002 für *«Informationssicherheitsmanagement (ISMS)»*. Datenschutz-Audits können in die Überprüfungsverfahren dieser Standards integriert werden und wo notwendig noch zusätzlich ergänzt werden.

Folgende Punkte sind in Bezug auf die Anwendbarkeit von ausländischen und/oder nationalen Datenschutzbestimmungen zu prüfen:

- ☐ Angebot von Produkten und Dienstleistungen in der EU oder im EWR
- ☐ Bearbeitung von Kunden in der EU oder im EWR
- ☐ Verhaltensbeobachtung von Personen in der EU oder im EWR
- ☐ Internetangebote/Publikationen für Personen in der EU oder im EWR
- ☐ Tochtergesellschaft, Niederlassung, Agent oder Zweigniederlassung in der EU oder im EWR

Mögliche Prüfungsbereiche

- ☐ Datenschutzerklärung und Nutzungsbedingungen Internetseite
- ☐ Bestehende Privacy Policy / Datenschutzweisungen
- ☐ Bestehende Datenschutzklauseln in Verträgen und allgemeinen Geschäftsbedingungen
- ☐ Übersicht über Datenbearbeitungen, Applikationen und Prozesse
- ☐ Rechtsgrundlage für die Bearbeitung von Personendaten
- ☐ Einwilligung in die Bearbeitung von Daten
- ☐ Prozesse für die Erfüllung der Betroffenenrechte (Auskunft, Löschung etc.)
- ☐ Beschäftigtendatenschutz
- ☐ Zulässigkeit einer Datenweitergabe an Dritte
- ☐ Auftragsverarbeiter – erforderliche Vereinbarungen
- ☐ Anforderungen an Datenübermittlung in Drittländer
- ☐ Pflicht zur Führung von Verarbeitungsverzeichnissen (Verantwortlicher und/oder Auftragsverarbeiter)
- ☐ Notwendigkeit für die Ernennung eines betrieblichen Datenschutzbeauftragten
- ☐ Notwendigkeit für die Ernennung eines Vertreters in der EU
- ☐ Meldungen an die zuständigen und/oder betroffenen Datenschutzaufsichtsbehörden
- ☐ Prozess «Data Breach Notification»
- ☐ Notwendigkeit einer Datenschutz-Folgeabschätzung
- ☐ Dokumentation technischer und organisatorischer Massnahmen (Datensicherheit)
- ☐ Prüfung von Zertifizierungen
- ☐ Regelung der elektronischen und physischen Archivierung

4. Leitlinien zur Durchführung eines Datenschutz-Compliance-Audits

Mit einem Audit soll die umfassende Einhaltung der schweizerischen und der europäischen Datenschutzbestimmungen im Unternehmen überprüft werden. Dabei werden folgende Zielsetzungen verfolgt:

- Review von Prozessen, Dokumenten oder funktionellen Bereichen betreffend die Umsetzung und Einhaltung der anwendbaren Datenschutzbestimmungen;
- Identifikation von Bereichen mit Verbesserungsmöglichkeiten;
- Auditbericht mit Bewertung und Empfehlungen;
- Management Reporting.

Ein wirksamer Audit wird mit einer Kombination von Dokumentenanalyse und Interviews mit den Verantwortungsträgern erreicht. Entsprechend wichtig ist es daher, diese mit einer transparenten Information in den Prozess einzubeziehen. Es muss dabei eine Kultur etabliert werden, in welcher die Beteiligten den Audit als Chance verstehen und Abweichungen oder Mängel ohne negative Wahrnehmung offengelegt werden können.

Als Erfolgsfaktoren dafür sind sicherzustellen, dass:

- die Auditprinzipien bei allen Auditbeteiligten ausreichend bekannt sind;
- ein gemeinsames Verständnis über diese Auditprinzipien besteht;
- ein Verständnis besteht, wie mit Fehlern, Mängeln und Abweichungen in der Organisation umgegangen wird.

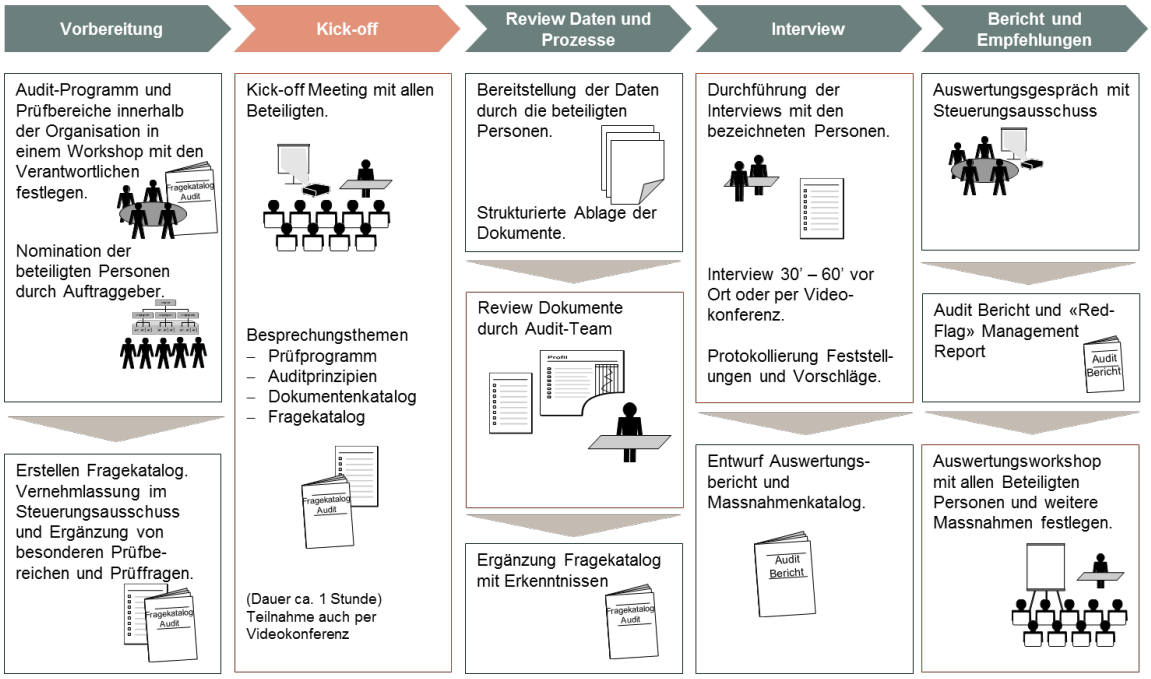
Falls es im Unternehmen noch keine gemeinsam vereinbarten Auditprinzipien gibt, kann der Standard ISO 19011 weiterhelfen. In Kapitel 4 der Norm sind einige Auditprinzipien beispielhaft aufgeführt und erläutert:

- Integrität als Grundlage der Professionalität.
- Sachliche Darstellung als Pflicht wahrheitsgemäss und genau zu berichten.
- Angemessene berufliche Sorgfalt durch Anwendung von Sorgfalt und Urteilsvermögen beim Auditieren.
- Vertraulichkeit hinsichtlich der Sicherheit von Informationen.
- Unabhängigkeit als Grundlage für Unparteilichkeit und Objektivität der Auditschlussfolgerungen.
- Faktengestützter Ansatz als rationale Methode, um zu zuverlässigen und nachvollziehbaren Auditschlussfolgerungen in einem systematischen Auditprozess zu kommen.
- Risikobasierter Ansatz, welcher Risiken und Chancen berücksichtigt.
- Auditprinzipien sind eine wichtige Voraussetzung für die Planung und Durchführung von Audits, weil sie allen Auditbeteiligten Regeln und ein Wertesystem für einen erfolgreichen Auditprozess geben und somit den respektvollen Umgang aller Auditbeteiligten miteinander unterstützen.

5. Vorgehen in fünf Schritten

Der Audit basiert auf einer Review der relevanten Dokumente sowie auf Interviews mit den verantwortlichen Personen. In den Interviews werden Detailfragen geklärt oder auch erkannte Problemfelder bereits identifiziert sowie Lösungsansätze diskutiert. Dies stellt sicher, dass im Report konkrete Beurteilungen und Massnahmen vorgeschlagen werden können.

Der Vorgehensplan für den Audit sieht fünf Phasen vor:



Der Aufwand ist bei der erstmaligen Durchführung etwas grösser. Bei der jährlichen Durchführung wird primär auf eine schriftliche Erhebung abgestützt; und nur noch kritische Punkte oder Neuerungen werden im Interview vertieft.

6. Fazit

Dem Unternehmen obliegt neu der Nachweis der Einhaltung der Datenschutzvorschriften. Der Umfang der Umsetzung und die jährliche Überprüfung sind jedoch nicht einheitlich festgelegt. Die Massnahmen müssen (nur) angemessen sein und sind daher spezifisch für das Unternehmen festzulegen. Es ist also zunächst das Risiko für die Rechte und Freiheiten der natürlichen Personen unter Berücksichtigung der Eintrittswahrscheinlichkeit festzustellen. Werden beispielsweise nur wenige personenbezogene Daten verarbeitet, die zudem keine sensiblen Informationen beinhalten, dann sind die Anforderungen an die getroffenen Massnahmen entsprechend niedriger. Dieser Nachweis und damit die regelmässige Dokumentation und Prüfung obliegt dem Unternehmen.

Bratschi AG unterstützt Sie bei der Umsetzung und Anwendung der Datenschutzregulierungen in Ihrem Unternehmen mit folgenden Dienstleistungen:

- Workshops zur Erhebung der Relevanz und der Handlungsfelder für die Umsetzung der neuen Datenschutzregulierungen;
- Projektbegleitung bei der Implementierung von Datenschutz-Management-Systemen;
- Schulungen und Trainings zum Datenschutz;
- Durchführung von Datenschutzaudits;
- Umsetzung von Datenschutzbestimmungen für Verträge oder Internetseiten;
- Verträgen, Einwilligungen.

Datenschutz sicher und erfolgreich umsetzen:

Anwendbarkeit der EU DSGVO in der Schweiz: Ein Datenschutzleitfaden für Schweizer Unternehmen.

Markus Näf, WEKA Business Media AG (www.weka.ch)

ISBN 978-3-297-02126-2.

Basel
Lange Gasse 15
Postfach
CH-4052 Basel
Telefon +41 58 258 19 00
Fax +41 58 258 19 99
basel@bratschi.ch

Bern
Bollwerk 15
Postfach
CH-3001 Bern
Telefon +41 58 258 16 00
Fax +41 58 258 16 99
bern@bratschi.ch

Lausanne
Avenue Mon-Repos 14
Postfach 5507
CH-1002 Lausanne
Téléfone +41 58 258 17 00
Téléfax +41 58 258 17 99
lausanne@bratschi.ch

St. Gallen
Vadianstrasse 44
Postfach 262
CH-9001 St. Gallen
Telefon +41 58 258 14 00
Fax +41 58 258 14 99
stgallen@bratschi.ch

Zug
Industriestrasse 24
CH-6300 Zug
Telefon +41 58 258 18 00
Fax +41 58 258 18 99
zug@bratschi.ch

Zürich
Bahnhofstrasse 70
Postfach
CH-8021 Zürich
Telefon +41 58 258 10 00
Fax +41 58 258 10 99
zuerich@bratschi.ch