DSGVO – Folgen für die Informationssicherheit

Am 25. Mai war es so weit und die Datenschutz-Grundverordnung der EU trat nach einer zweijährigen Übergangsfrist in Kraft. Dieser Blog-Artikel gibt einen Einblick auf die Folgen für die Informationssicherheit.

Die neue Datenschutz-Grundverordnung hat das Ziel, eine einheitliche, EU-weite Regelung in Bezug auf die Verarbeitung von personenbezogenen Daten sicherzustellen. Dies gilt für alle Unternehmen, die Dienstleistungen in der EU anbieten, unabhängig davon, ob sie einen Sitz innerhalb oder ausserhalb der Europäischen Union haben. Wie die einzelnen Verordnungsartikel zustande kamen, zeigen die 173 Erwägungsgründe. Diese sind ein guter Anlaufpunkt, falls bei der Umsetzung unklar ist, welches Ziel der Gesetzesgeber genau dabei verfolgt hat.

Anwendungsbereich

Wie erwähnt gilt die DSGVO für die Verarbeitung personenbezogener Daten. Es spielt dabei keine Rolle, ob dies automatisiert oder nicht automatisiert erfolgt. Bei der Verarbeitung ist es auch unabhängig davon, ob die Daten elektronisch oder zum Beispiel auf Papier verarbeitet werden.

Was sind aber personenbezogene Daten? In Artikel 4, Nr. 1 steht: «alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (im Folgenden betroffene Person) beziehen; als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind, identifiziert werden kann».

Beispiele dafür sind Name, Wohnort, Geburtsdatum, Personalnummer, Parteizugehörigkeit usw. Explizit steht hier «natürliche Personen», das heisst, es bezieht sich somit nicht auf Firmen. Jedoch hat der Gesetzesgeber 69 Öffnungsklauseln zugelassen. Österreich hat dies genutzt und hier auch juristische Personen mit einbezogen. Bei der Verarbeitung sind sowohl das Erheben (Daten beschaffen), Speichern, Ändern, Übermitteln, Verknüpfen (mit anderen Daten) oder auch Löschen gemeint. Das bedeutet, es spielt keine Rolle, wer was mit den Daten anstellt. Die Ausnahme bilden nur persönliche oder familiäre Bearbeitungen.

Verzeichnis von Verarbeitungstätigkeiten

In einem ersten Schritt sollte ein Verzeichnis von Verarbeitungstätigkeiten erstellt werden. In Artikel 30 ist ausführlich beschrieben, was darin zu erfassen ist. Es sind dies:

- Namen und Kontaktdaten des/der Verantwortlichen
- Zweck der Verarbeitung
- Erfasste Kategorien
- Empfänger der Daten, allenfalls Angabe der Drittländer
- Übermittlung der Daten, inklusiv allfälliger Drittländer
- Fristen zur Löschung der Daten
- Beschreibung der technischen und organisatorischen Massnahmen (TOM)

Weiter wird verlangt, dass dies schriftlich zu erfolgen hat. Ausnahmen sind nur für Unternehmen, die weniger als 250 Mitarbeiter beschäftigen und die nur gelegentlich eine Verarbeitung der Daten vornehmen, erlaubt.

Da vermutlich kein Unternehmen nur gelegentlich eine Verarbeitung vornimmt, gilt diese Pflicht für alle Unternehmen. Als Tipp sollten auch Änderungen an diesem Verzeichnis gespeichert werden. So ist es für die Datenschutzaufsichtsbehörde sichtbar, was, wann von wem geändert wurde.

Grundsätze der Verarbeitung von personenbezogenen Daten

Grundsätzlich ist es nicht erlaubt, mit personenbezogenen Daten zu arbeiten. Entweder gibt es dazu eine Rechtsgrundlage oder ich habe die Einwilligung für diese Datenbearbeitung. Diese Einwilligung muss freiwillig sein und wird für einen bestimmten Zweck abgegeben (Zweckbindung). Die betroffene Person muss klar und verständlich über den Verwendungszweck und über einen Wi-

derruf informiert worden sein. Beispielsweise kann dies eine schriftliche Erklärung oder das Ankreuzen eines Feldes sein (Achtung: dieses Kreuz darf nicht vorausgefüllt sein). Für ein Unternehmen ist es wichtig, diese Einwilligung revisionssicher aufzubewahren.

Werden die erhobenen Daten nicht mehr benötigt und es gibt auch keine Aufbewahrungsvorschriften mehr, müssen die Daten gelöscht oder so verändert werden, dass kein Personenbezug mehr möglich ist.

IT-Sicherheit

Der Artikel 32 DSGVO erwähnt die klassischen Schutzziele der Informationssicherheit: «Unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen treffen der Verantwortliche und der Auftragsverarbeiter geeignete technische und organisatorische Massnahmen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten.»

Weiter wird ausgeführt, was dies beinhalten sollte:

- die Pseudonymisierung und Verschlüsselung personenbezogener Daten;
- die Fähigkeit, die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherzustellen;
- die Fähigkeit, die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen;
- ein Verfahren zur regelmässigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Massnahmen zur Gewährleistung der Sicherheit der Verarbeitung.

Schauen wir uns die Punkte genauer an:

Pseudonymisierung

Der Artikel 4 der DSGVO beschreibt dies wie folgt: «die Verarbeitung personenbezogener Daten in einer Weise, dass die personenbezogenen Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und technischen und organisatorischen Massnahmen unterliegen, die gewährleisten, dass die personenbezogenen Daten nicht einer identifizierten oder identifizierbaren natürlichen Person zugewiesen werden».

Für eine Datenbank könnte dies beispielsweise ein Hash-Wert sein. Dieser ist nicht umkehrbar. Von Vorteil wird ein sicheres Verfahren wie SHA-2 oder SHA-3 verwendet. MD5 und SHA-1 gelten nicht mehr als sicher, da bereits erfolgreiche Angriffe darauf stattgefunden haben.

Verschlüsselung

Die Verschlüsselung kann auf verschiedene Arten eingesetzt werden.

– E-Mail-Server: Gemäss dem Bayrischen Landesamt für Datenschutzaufsicht genügt es bereits, auf dem E-Mail-Server STARTTLS und Perfect Forward Secrecy zu verwenden. Dabei kommunizieren die Server untereinander verschlüsselt. Die Verbindung zwischen dem sendenden und empfangenden Server ist damit für einen Dritten nicht einsehbar, das heisst der Transport der Nachricht ist geschützt.
– Webseite: Auf einer Webseite muss zwingend HTTPS verwendet werden. Die Daten sind dabei für einen Dritten nicht einsehbar, der sich in die Verbindung einschleichen will. Auch für Kontaktformulare muss die sichere Variante verwendet werden.
– Dateien, Dokumente und Nachrichten: ein einfaches Verfahren ist es, die Dateien/Dokumente direkt zu verschlüsseln. 7-ZIP wäre ein Programm, welches die Daten sicher verschlüsseln kann (beispielsweise mit AES-256). Bei E-Mails kommen S/MIME oder PGP zum Einsatz (beide Technologien werden in einem weiteren Blog-Artikel ausführlich beschrieben).
– Cloud: Daten in der Cloud sind nicht verschlüsselt, auch wenn der Transport der Daten in der Regel über HTTPS erfolgt. Der Cloud-Anbieter kann jederzeit auf die Daten zugreifen. Diesem Umstand gilt es grosse Beachtung zu schenken. Die Daten sollten daher immer verschlüsselt abgelegt werden, dies unabhängig, ob das Rechenzentrum in der Schweiz oder der EU liegt. Eine Variante ist die Software Boxcryptor. Sie stellt eine Mittelschicht zwischen lokalem Rechner und Cloud-Dienstleister zur Verfügung (unter Windows das Laufwerk X, auf einem Mac ein zusätzliches Laufwerk). Alle Daten, die via diesem Laufwerk abgespeichert werden, sind verschlüsselt. Für Boxcryptor spielt es keine Rolle, ob dies OneDrive, Google Drive, Dropbox oder ein anderer Anbieter ist.
– WLAN: Auch WLAN-Netzwerke sind zwingend sicher zu betreiben. WPA2 sowie ein gutes Passwort (Empfehlung BSI mindestens 20 Stellen) müssen unbedingt verlangt werden. Voreingestellte Passwörter sind umgehend zu ändern (oft auf dem Boden aufgeklebt).
– VPN: der entfernte Zugriff auf Daten muss ebenfalls verschlüsselt sein. Achten Sie hier auf aktuelle Algorithmen, um die Sicherheit zu gewährleisten.
– Mobile Geräte: egal ob es sich um Handys, Tablets oder Laptops handelt, alle Geräte sind zu verschlüsseln. Dabei genügt es bereits, die vom Hersteller implementierten Funktionen zu nutzen. Alternativen wie VeraCrypt können ebenso verwendet werden (BSI-Empfehlung).

CIA

Die Norm spricht explizit die Sicherheitsziele Vertraulichkeit, Integrität und Verfügbarkeit an. Zudem wird die Belastbarkeit der Systeme verlangt. Ein Unternehmen muss dies auf die Dauer sicherstellen können. Die Vertraulichkeit kann beispielsweise mit der bereits erwähnten Verschlüsselung garantiert werden. Aber auch ein sauberes Access-Management gehört dazu. Es sollte das Least Privilege-Prinzip gelten, das heisst nur die Rechte bekommen, die auch für die alltägliche Arbeit benötigt werden. Es gibt keinen Grund, warum ein Mitarbeiter zum Beispiel ständig mit administrativen Rechten arbeiten muss. Die Integrität kann mit diesen Vorgaben ebenfalls positiv beeinflusst werden. Bei der Integrität können auch Checksummen von Daten und Logs helfen. Die Logs zwar nur indirekt, aber es ist dann feststellbar, wer wann was geändert hat. Die Verfügbarkeit kann durch redundante Systeme, redundante Speicher, aber auch mit einer passenden Backup-Strategie sichergestellt werden.

Wiederherstellung/Backup

Die DSGVO verlangt, dass die personenbezogenen Daten, inklusiv Zugang bei physischen oder technischen Zwischenfällen rasch wiederhergestellt werden können. Dazu muss eine den Anforderungen angepasste Backup-Strategie erstellt werden. Auch ein Business Continuity sollte in Betracht gezogen werden. Das BCM kommt bei einem grösseren Vorfall zum Zuge

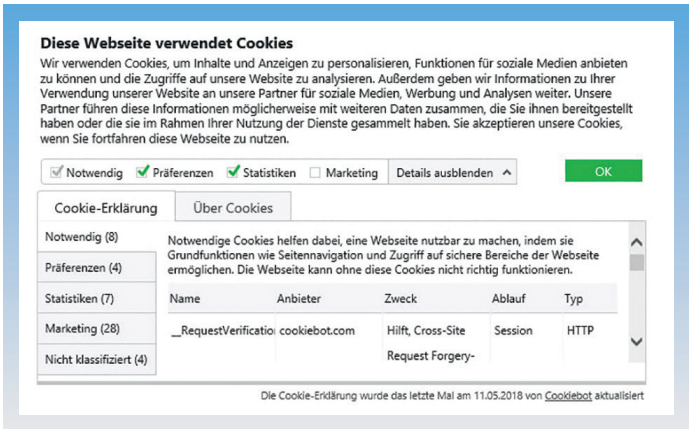

Bild 1.

und hilft, nach einem Vorfall schnell wieder produktiv arbeiten zu können. Wie so ein Backup-Konzept aussehen könnte, folgt in einem weiteren Blog-Beitrag.

Patch-Management

Jede Software hat Schwachstellen. Daher ist es wichtig, wenn Schwachstellen erkannt werden, schnell und angepasst darauf reagieren zu können. In einem ersten Schritt sollte das Risiko dieser Schwachstelle bewertet werden. Sind Sofortmassnahmen notwendig? Oder kann dies im gewohnten Patch-Rhythmus (zum Beispiel monatlich) erfolgen? Entweder erfolgt ein ausserordentlicher Termin oder während des Wartungsfensters wird die Schwachstelle durch den Patch (Software, welche die Schwachstelle behebt) beseitigt.

Regelmässige Überprüfung

Weiter steht im Artikel 32, dass mittels eines zu definierenden Verfahrens regelmässige Überprüfungen, Bewertungen und Evaluierung der Wirksamkeit der technischen und organisatorischen Massnahmen erfolgen muss. Es genügt also nicht, einmal eine Massnahme umzusetzen und danach nichts mehr. Diese Kontrollen sind unbedingt schriftlich festzuhalten: Welches Resultat wurde erzielt? Welche Schwächen erkannt? Welche Schritte wurden eingeleitet? Dabei kann auch auf externe Unterstützung gesetzt werden. Zum Beispiel meine Firma, die goSecurity GmbH, kann hier in einem Audit aufzeigen, wo allenfalls Verbesserungspotenzial vorhanden ist.

Physische Sicherheit

Auch die physische Sicherheit ist wichtig. So darf es nicht sein, dass jemand einfach in ein Gebäude oder Büro reinlaufen und personenbezogene Daten mitnehmen kann. Diese Daten sollten nach Bearbeitung immer verschlossen aufbewahrt werden. Arbeitsgeräte sind immer zu sperren, damit niemand «Fremdes» auf die Daten zugreifen kann.

Artikel 25 verlangt, dass bereits im Vorfeld datenschutzfreundlich geplant und definiert wird. Oft liest und hört man dann von Privacy by Design und Privacy by Default.

Privacy by Design

Bei Privacy by Design ist gemeint, dass bereits im Vorfeld technische Massnahmen zum Schutz der personenbezogenen Daten ergriffen wurden. Dies können zum Beispiel verschlüsselte Datenbanken sein. Ohne passenden Schlüssel kann niemand die Daten auslesen. Weitere Möglichkeiten sind:

Login gekoppelt mit Windows-Login

Es wird nur ein Login für alle Dienste benötigt. Somit kann im Hintergrund die Konfiguration und Steuerung übernommen werden. Beispielsweise können Gruppen oder Rollen definiert werden. Ein Benutzer wird nun einer Rolle zugeteilt und erbt alle damit verbundenen Rechte. Weiter ist die Nachvollziehbarkeit damit einfacher möglich.

Passwortanforderungen erhöhen

Passwörter sind immer wieder eine grosse Herausforderung. Es darf aber nicht sein, dass einfache Passwörter wie 1234 zugelassen

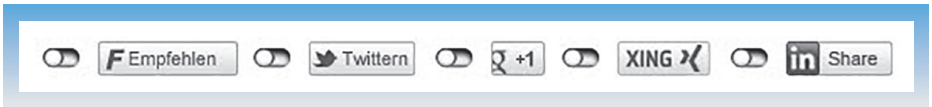

Bild 2.

sind. In Weisungen sollte allen auf eine einfache Art und Weise erklärt werden, wie sichere Passwörter erstellt und (im Kopf) behalten werden können. Anschliessend müssen die Systeme dies auch so durchsetzen und verlangen.

Zugriffsbeschränkungen
Wie bereits erwähnt, sollten nur die Rechte vergeben werden, die auch für die alltägliche Arbeit benötigt werden.

Pseudonymisierung
Die personenbezogenen Daten sollten in eine Form gebracht werden, wo ein direkter Bezug zur echten Person nicht mehr möglich ist. Zum Beispiel bei Google Analytics kann eine Option aktiviert werden, damit nicht die komplette IP-Adresse gespeichert wird.

Cookies

In der EU ist auch eine Cookie-Richtlinie vorhanden. Diese wird im Zuge der neuen Verordnung gerade überarbeitet. Vermutlich Ende dieses Jahres oder Anfang des kommenden Jahres tritt diese in Kraft. Ohne Einwilligung dürfen keine Cookies gesetzt werden. Dies technisch umzusetzen ist gar nicht so einfach. Damit dies rechtskonform erfolgt, hat die EU unter http://ec.europa.eu/ipg/basics/legal/cookies/ eine mögliche Lösung hinterlegt. Alternativ könnte der CookieBot von www.cookiebot.com/de/ eingesetzt werden. Bild 1 wird dann präsentiert. Hier ist auf einen Blick ersichtlich, welche Cookies, für was und wie lange dieses gespeichert wird, ersichtlich. Einzelne Cookies können gruppenweise deaktiviert werden.

Wer gar nicht erst Cookies auf dem Rechner haben möchte, nutzt ein Plugin im Browser (Ghostery, NoTrack oder ähnliche).

Nervend sind auch die Spuren, die man bei Facebook, Google und anderen Diensten hinterlässt. Der Grund sind oft Webseitenbetreiber, die den Like/Teilen- usw. Button direkt einbinden. Der Heise-Verlag hat hier ein Projekt lanciert, dass dies verhindert. Nun muss jedoch zwei Mal geklickt werden. Zuerst, um den Button zu aktivieren und danach, um den Like abzusetzen. Beim Besuch der Webseite sieht es so aus (Bild 2). Nach einem Klick dann so (Bild 3). Weitere Infos sind unter www.heise.de/ct/artikel/2-Klicks-fuer-mehr-Datenschutz-1333879.html verfügbar.

Bild 3.

Privacy by Default

Hier sind die datenschutzkonformen Einstellungen gemeint. Wenn ich Informationen von einem Unternehmen möchte, darf das Häkchen «ich bestelle auch gleich den Newsletter» NICHT gesetzt sein. Der Kunde muss explizit dazu einwilligen. Weiter sollten nur die Daten erfasst werden, die auch benötigt werden. Warum wird ein Geburtsdatum für den Newsletter benötigt? Falls Sie gerne eine Geburtstagskarte schicken möchten, dann schreiben Sie dies hin, aber machen Sie dieses Feld zur freiwilligen Eingabe.

Leider ist anhand der Formulierung nicht klar, wie weit diese beiden Anforderungen gehen müssten. Die Rechtsprechung wird in den kommenden Wochen und Monaten zeigen, wie weit die EU hier gehen möchte. Es gilt daher, dieses Thema stetig im Auge zu behalten.

Dieser Artikel hat nur einige wenige Dinge auf der technischen Seite gezeigt. Die Rechte des Kunden (zum Beispiel das Recht auf Vergessen), die Pflicht für einen Datenschutzbeauftragten, die Reaktion bei Vorfällen und andere Themen wurden nicht beleuchtet. Besonders in der Schweiz herrscht eine grosse Unsicherheit, in wie weit das eigene Unternehmen wirklich davon betroffen ist oder nicht. Nichtsdestotrotz sollte sich jedes Unternehmen mit der DSGVO auseinandersetzen. Alles, was eine Aussenwirkung hat (Homepage, Werbung, HR-Prozess usw.) muss konform sein. Dabei sollte sich jedes Unternehmen immer wieder überlegen: welche Daten benötigen wir wirklich? Und wie schützen wir die erhobenen Daten effektiv? Datensparsamkeit ist ein guter Vorsatz, um die angedrohten Bussen bis 20 Millionen oder 4 Prozent des weltweiten Umsatzes nicht zu spüren zu bekommen.

INFOS | KONTAKT

goSecurity GmbH
Schulstrasse 11
CH-8542 Wiesendangen

Telefon +41 (0)52 511 37 37
www.goSecurity.ch
wisler@gosecurity.ch