DATENSCHUTZ FÜR DIGITALE GESCHÄFTSMODELLE

Was muss man im
Bereich Datenschutz beachten?

INHALTSVERZEICHNIS

Hinweis:
Dieser Leitfaden soll Ihnen zur Anregung dienen. Er erhebt keinen Anspruch auf Vollständigkeit. Es ersetzt auch keine rechtliche Beratung oder eine individuelle Datenschutzberatung.

Anhand dieser Checkliste ist es leichter herauszufinden, in welchen Bereichen des Datenschutzes Sie aktiv werden sollten. Verschaffen Sie sich zu Beginn einen Überblick:

- Was ist wichtig und was muss ich tun?
- Die DSGVO unterscheidet nicht nach Größe eines Unternehmens, sondern nach Art der Daten und nach den Verarbeitungstätigkeiten. Was bedeutet das nun für mich?
- Die Suche nach seriösen Quellen. Am umfangreichsten ist hier wohl die Sammlung des Bayrischen Landesamtes für Datenschutzaufsicht. Hier gibt es auch einen Selbsttest.

Danach kommt die Strukturierung. Wie gehen Sie vor? Erfahrungsgemäss braucht es mindestens zwei Woche, um die einzelnen Schritte zu gehen. Viel Zeit beansprucht die Recherche und die genaue Definition der Prozesse in Ihrem Unternehmen.

Digitale Geschäftsmodelle
Digitale Geschäftsmodelle sind Unternehmen, die stark digitalisierte Prozesse haben und ein Bedürfnis für Zielgruppen erfüllen.

Hierbei gibt es verschiedene Geschäftsmodelle im Überblick:
- Ecommerce: Elektronischer Handel mit materiellen Gütern
- Plattformen: Verknüpfung mit Marktleuten
- Fremium: Basisprodukt gratis, Vollprodukt kostenpflichtig
- Subscription: Mitglieder- und Abo-Prinzip
- Pay-per-Use: Zahlung für Verbrauch
- Daten: Handeln und Nutzung relevanter Daten

Beispiele sind Softwareentwickler, aber auch Portale, digitale Marketingagenturen, Personalvermittler, etc.

Personenbezogene Daten sind alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen (Art. 4 DSGVO)

Grundsätzlich

sind die Erhebung, Verarbeitung und Speicherung von personenbezogenen Daten verboten. Diese Datenvorgänge dürfen nur erfolgen, wenn eine Einwilligung besteht, ein Vertrag vorliegt, der dies vorsieht, bzw. man sich in einer vorvertraglichen Anbahnung befindet, eine Interessenabwägung durchgeführt wurde oder andere Rechtsvorschriften bzw. Erfüllung rechtlicher Pflichten dies erlauben. Betroffene haben vor allem das Recht auf informationelle Selbstbestimmung.

Werden in Ihrem Unternehmen Daten wie:

☐ Name
☐ Adresse
☐ Kontaktdaten
☐ Bankdaten
☐ Kreditkartennummer
☐ Sozialversicherungsnummer
☐ Löhne oder Gehälter
☐ IP Adressen
☐ Standortdaten

genutzt bzw. verwendet?

Dies ist keine vollständige Aufzählung. Es soll Ihnen lediglich als Denkanstoß dienen. Bestimmt haben Sie noch mehr Arten von Daten. Falls diese ähnlich sind, fallen sie auch in diese Kategorie. Es können Daten von Interessenten, Kunden, Mitarbeitern, Lieferanten oder Dienstleistern sein.
Wenn Sie diese Arten von Daten erheben, verarbeiten oder speichern, dann liegt es in Ihrer Verantwortung, diese Daten zu schützen.

Besondere personenbezogene Daten

Diese Kategorie von Daten ist besonders schutzbedürftig. Es geht um Daten wie:

☐ rassistische oder ethische Herkunft
☐ politische Meinung
☐ religiöse oder philosophische Überzeugung
☐ Gewerkschaftszugehörigkeit
☐ Daten die Gesundheit oder Sexualleben betreffen
☐ Vermögensverhältnisse
☐ Vorstrafen und laufende Ermittlungsverfahren betreffend
☐ genetische Daten
☐ biometrische Daten

Sind Sie unsicher? Wir unterstützen Sie gerne.

Erhebung personenbezogener Daten

Hier ist die Frage, ob Sie die Daten direkt von der betroffenen Person erhalten oder über Dritte. Erhalten Sie die Daten direkt, so muss die Rechtsgrundlage (Art. 6 –DSGVO) klar und verständlich sein.

Erhalten Sie die Daten direkt, so muss die Rechtsgrundlage (Art. 6 –DSGVO) klar und verständlich sein. Laut Art. 6 DSGVO ist die Verarbeitung personenbezogener Daten rechtmäßig,
- wenn eine Einwilligung der betroffenen Person vorliegt,
- zur Erfüllung eines Vertrages oder zur Durchführung vorvertraglicher Maßnahmen,
- zur Erfüllung einer rechtlichen Verpflichtung
- zum Schutze lebenswichtiger Interessen,
- zur Wahrnehmung einer Aufgabe, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt oder
- aufgrund einer Interessenabwägung erforderlich ist.

Die Datenverarbeitung ist bereits dann rechtmäßig, wenn einer der genannten Tatbestände vorliegt. Im Grundsatz bleibt daher alles verboten, was nicht ausdrücklich erlaubt ist.

Erhalten Sie die Daten von Dritten und bearbeiten oder/und speichern diese, dann sollten Sie abklären, ob Sie eine Auftragsverarbeitung durchführen. Sie müssen sich um den Datenschutz kümmern. Bei der Auftragsverarbeitung müssen Sie einen Vertrag mit Ihrem Auftraggeber schließen und technische und organisatorische Maßnahmen zum Schutze der Daten durchführen.

Grundsätzlich gilt: Wer personenbezogene Daten verarbeitet, muss diese mittels technischer und organisatorischer Maßnahmen (TOM) schützen.

Unter technischen Maßnahmen sind alle Schutzversuche zu verstehen, die im weitesten Sinne physisch umsetzbar sind, wie zum Beispiel:

Erhebung personenbezogener Daten

Hier ist die Frage, ob Sie die Daten direkt von der betroffenen Person bekommen oder über Dritte. Erhalten Sie die Daten direkt, so muss die Rechts-grundlage (Art. 6 –DSGVO) klar und verständlich sein.

- Sicherung von Türen und Fenstern
- Alarmanlagen jeglicher Art
- Maßnahmen die in Soft- und Hardware umgesetzt werden, wie etwa
  - Benutzerkonto
  - Passworterzwingung,
  - Login (Protokolldateien),
  - biometrische Benutzeridentifikation

Als organisatorische Maßnahmen sind solche Schutzversuche zu verstehen die durch Handlungsanweisung, Verfahrens- und Vorgehensweisen umgesetzt werden.

Beispiele:

- Besucheranmeldung
- Arbeitsanweisung zum Umgang mit fehlerhaften Druckerzeugnissen
- Vier-Augen-Prinzip
- festgelegte Intervalle zur Stichproben Prüfungen

Die entsprechenden Vorschriften zur Auftragsverarbeitung finden dabei schon dann Anwendung, wenn die Verarbeitung einen Zusammenhang mit Tätigkeiten einer Niederlassung in der Union aufweist.

Unsere Empfehlung:
Besprechen Sie diese Punkte mit einem Datenschutzbeauftragten.
Wir stehen Ihnen gerne zur Verfügung.

Mindestanforderungen an den Auftragsverarbeitungsvertrag

Nach Art. 4 Nr. 8 DSGVO ist ein Auftragsverarbeiter eine Stelle, die personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet. Der Verantwortliche ist gemäß Art. 4 Nr. 7 DSGVO die Stelle, die allein oder gemeinsam mit anderen über die Mittel und Zwecke der Verarbeitung personenbezogener Daten entscheidet. Hierbei kommt es maßgeblich auf die Entscheidung über die Verarbeitungszwecke an, während die Entscheidung über die technisch-organisatorischen Fragen der Verarbeitung auch auf den Auftragsverarbeiter delegiert werden kann.

Der Art. 28 Abs. 3 DSGVO gibt dabei dessen inhaltliche Mindestanforderungen vor. Folgende Inhalte müssen im Vertrag zur Auftragsverarbeitung stehen:

- Welche Art von personenbezogenen Daten wird verarbeitet
- die Dauer der Verarbeitung
- Art der personenbezogenen Daten und Kategorien von betroffenen Personen
- Pflichten und Rechte des Verantwortlichen und was Gegenstand und was Zweck der Verarbeitung sind
- Umfang der Weisungsbefugnisse
- Verpflichtung der zur Verarbeitung befugten Personen zur Vertraulichkeit
- Sicherstellung von technischen und organisatorischen Maßnahmen für den Datenschutz (TOM)
- Ob und welche Subunternehmer beauftragt werden dürfen
- Unterstützung des Auftraggebers bei Anfragen und Ansprüchen Betroffener sowie bei der Meldepflicht bei Datenschutzverletzungen
- Pflicht des Auftragsverarbeiters, den Verantwortlichen zu informieren, falls eine Weisung gegen Datenschutzrecht verstößt
- Dass personenbezogene Daten gelöscht und zurückgegeben werden müssen nach Abschluss der Auftragsdatenverarbeitung
- Kontrollrechte des für die Verarbeitung Verantwortlichen und Duldungspflichten des Auftragsverarbeiters.

Auftragsverarbeitung –externe Dienstleister

Die Auftragsverarbeitung ist die Erhebung, Verarbeitung oder Nutzung von personenbezogenen Daten durch einen Auftragsverarbeiter gemäss den Weisungen des für die Datenverarbeitung Verantwortlichen auf Grundlage eines Vertrages.

Bei der Auftragsverarbeitung durch externe Dienstleister haben viele Unternehmen Probleme.
Es deutet auf eine Auftragsverarbeitung hin, wenn der Auftragnehmer:

- keine Entscheidungsbefugnis über die Daten hat
- keinen eigenen Geschäftszweck verfolgt bezüglich der personenbezogenen Daten
- einem Nutzungsverbot der zu verarbeitenden Daten unterliegt
- in keiner vertraglichen Beziehung zu den Betroffenen steht, die er verarbeitet
- und nach außen hin der Auftraggeber für die Datenverarbeitung verantwortlich ist

Beispiel für eine Auftragsverarbeitung durch externe Dienstleister ist die Weitergabe der personenbezogenen Daten an Dritte (Bsp. Speichern in der Cloud, Email-Newsletter-Versand, Buchhaltung über Virtuelle Assistenz) oder wenn externe Dienstleister bei Ihnen vorbeischauen, wie zum Beispiel IT-Dienstleister.

Hierfür braucht man einen Vertrag zur Auftragsverarbeitung.
Aus diesem Vertragsverhältnis ergibt sich auch eine Kontrollpflicht des Auftraggebers. Wenn Sie einen externen Dienstleister beauftragen, legen Sie die Zwecke und Mittel der Datenverarbeitung fest. Sie sind verantwortlich für die Daten dem Betroffenen gegenüber.

Verarbeitung und Speicherung von personenbezogenen Daten

Wenn Sie eine Erlaubnis zur Verarbeitung und Speicherung von personenbezogenen Daten haben, dann schauen Sie sich das Verfahren genau an.

Stimmt der Zweck, der in der Erlaubniserklärung genannt ist, mit dem Zweck der Verarbeitung überein?

Sie dürfen die erhobenen Daten nicht einfach für andere Zwecke verwenden, wie bei folgendem Beispiel: Die Daten aus einer Bestellung, die für die Abwicklung der Bestellung gebraucht werden, dürfen nicht auch für Werbung genutzt werden.

Ein weiterer Punkt, der hier berücksichtigt werden muss, ist der Schutz der Daten bei der Verarbeitung und Speicherung:

- Hat jeder im Büro oder im Home-Office (theoretisch) Zugang?
- Wer hat Zutritt, Zugang und Zugriff auf die Daten?
- Werden sie verschlüsselt gespeichert?
- Wo werden die Daten gespeichert? Extern oder bei Ihnen auf dem PC?
- Wie ist Ihre IT-Infrastruktur aufgebaut? Haben Sie einen Firewall?
- Oder ein Antivirenprogramm?
- Werden regelmäßig Sicherheitsupdates durchgeführt?

Wie Sie sehen, gibt es hier eine Fülle an Fragen, die man sich stellen kann und sollte. Auch diese Aufzählung soll lediglich ein Denkanstoß sein.

Haben Sie ein Verzeichnis von Verarbeitungstätigkeiten?

Die Datenschutz-Grundverordnung verpflichtet Unternehmen nach Art. 30 EU-DSGVO dazu, eine schriftliche Dokumentation und Übersicht über Verfahren zu führen, bei denen personenbezogene Daten verarbeitet werden.

Die Pflicht zum Führen eines Verzeichnisses von Verarbeitungstätigkeiten trifft nicht nur den Verantwortlichen und seine Vertreter, sondern nach Art. 30 Abs. 2 DSGVO auch den Auftragsverarbeiter und dessen Vertreter direkt. Unternehmen oder Einrichtungen mit weniger als 250 Mitarbeitern sind nach Abs. 5 ausnahmsweise vom Führen eines Verzeichnisses befreit, wenn die vorgenommene Verarbeitung kein Risiko für die Rechte und Freiheiten der betroffenen Personen birgt, keine Verarbeitung besonderer Datenkategorien erfolgt oder die Verarbeitung nur gelegentlich erfolgt.
In der Praxis gibt es jedoch nur wenige Unternehmen, die hiervon wirklich befreit werden.
Im Verzeichnis von Verarbeitungstätigkeiten werden die Verfahren aufgelistet mit denen Daten erhoben, verarbeitet und gespeichert werden.

Folgende Daten muss das Verzeichnis enthalten:

1. Namen und Kontaktdaten des Verantwortlichen
   (und ggf. des gemeinsam mit ihm Verantwortlichen), des Vertreters und ggf. Datenschutzbeauftragten
2. Zwecke der Verarbeitung
3. Kategorien betroffener Personen und personenbezogener Daten
4. Kategorien von Empfängern
5. Ggf. Übermittlungen von personenbezogenen Daten an ein Drittland oder an eine internationale Organisation
6. Wenn möglich: Löschfristen der verschiedenen Datenkategorien
7. Wenn möglich: Technische und organisatorische Maßnahmen (TOM)

Haben Sie ein Verzeichnis von Verarbeitungstätigkeiten?

Wichtig dabei zu beachten ist, dass das Verzeichnis auch folgende Angaben zum Verantwortlichen enthalten muss:

- Angabe des Verantwortlichen (i.d.R. also Nennung des Unternehmens)
- Anschrift
- Vertretungsberechtigte Personen (bei der GmbH z.B. die Geschäftsführer)
- Angaben zum Datenschutzbeauftragten (soweit vorhanden)

Gerne sind wir Ihnen bei der Anpassung des Verzeichnisses behilflich.

Datenschutz-Folgenabschätzung DSFA

Mit Inkrafttreten der europäischen Datenschutzgrundverordnung (DSGVO) im Mai 2018 wird die Vorabkontrolle durch die Datenschutz-Folgenabschätzung nach Art. 35 abgelöst.
Das Ziel der DSFA ist es, vor der Einführung von automatisierten Verfahren, deren Gefahren für die Sicherheit der personenbezogenen Daten zu überprüfen. Dadurch soll sichergestellt werden, dass die Wahl bei der Nutzung von automatisierten Verfahren auch unter datenschutzrechtlichen Aspekten erfolgt. Dies muss immer dann erfolgen, wenn die automatisierten Verfahren besondere Risiken für die Rechte der Betroffenen beinhalten.

Ein Beispiel: Ein Unternehmen bietet einen CarSharing-Dienst oder andere Mobilitätsdienstleistungen an und verarbeitet hierfür insbesondere umfangreiche Positions- und Abrechnungsdaten.

Nach Art. 35 (2) DSGVO kann bei der Durchführung der Datenschutz-Folgenabschätzung der Datenschutzbeauftragte beraten. Außerdem besteht Dokumentationspflicht.

Informationspflicht bei Datenpannen
Manchmal geht es schneller als gedacht und man begeht unabsichtlich eine Datenschutzverletzung. Sei es ein verlorener USB-Stick mit Kundendaten, versehentlicher Versand einer Mail mit allen Kontaktdaten in cc anstatt in bcc oder auch durch einen externen Hackerangriff. Diese Beispiele sind Datenschutzverletzungen bzw. Datenpannen, die jedem passieren können. Doch was ist jetzt zu tun?

Nach Art. 33 DSGVO sind sogenannte Data Breaches unter Umständen der Aufsichtsbehörde und ggf. auch den Betroffenen anzuzeigen. Ich habe Ihnen die wichtigsten Schritte und Kriterien für die Meldung einer Datenpanne zusammengefasst.

Datenschutz-Folgenabschätzung DSFA

Wem müssen Sie eine Datenpanne melden?

- der Aufsichtsbehörde
- ggfs. den Betroffenen

Eine Meldung hat immer an die zuständige Aufsichtsbehörde des Verantwortlichen zu geschehen. In manchen Fällen, vor allem, wenn voraussichtlich ein hohes Risiko für die persönlichen Rechte und Freiheiten der Betroffenen vorliegt, muss eine Meldung ebenfalls an den/die Betroffenen geschehen. Ein hohes Risiko liegt dann vor, wenn die Schwere und die Eintrittswahrscheinlichkeit eines Schadens als sehr groß bewertet werden.

Auftragsverarbeiter (z. B. Mitarbeiter, Freelancer, freie Mitarbeiter) müssen Datenpannen stets an den Verantwortlichen melden.

Dieser leitet dann die weiteren Schritte ein.

Die Meldung muss unverzüglich, spätestens 72 Stunden nach Kenntnisnahme, erfolgen. Sollte die 72-Stunden-Frist nicht eingehalten werden, hat der Verantwortliche dies zu begründen. Hierbei müssen außergewöhnliche Umstände dargestellt werden. (z. B. wenn viele Hacker-Attacken in kurzer Zeit auftreten.) Wiederum besteht kein außergewöhnlicher Umstand, falls noch nicht alle geforderten Inhalte bekannt sind. Hier ist der Verantwortliche weiterhin in der Pflicht, die Meldung rechtzeitig zu vollziehen und fehlende Informationen später nachzureichen.

Die Meldepflicht besteht im „Falle einer Verletzung des Schutzes personenbezogener Daten“, „es sei denn, dass die Verletzung (…) voraussichtlich nicht zu einem Risiko führt.“ (Vgl. Art. 33 DSGVO)

Beispiele für Data Breaches:

- Hacking
- Datendiebstahl
- SQL-Lücken
- Bugs im Webserver
- Verlorengegangene USB-Sticks oder Laptops
- Unrechtmäßige Übermittlung
- Einbruch in Serverräumen (Verlust oder Zerstörung von Hardware, Auslesen von Datenträgern)
- Versehentliche Falschadressierung von Briefen und E-Mails
- Versenden von Massen-E-Mails unter Verwendung des cc- statt bcc-Feldes
- Vorübergehende Unerreichbarkeit der Daten (Stromausfall, Denial-of-Service-Attacke)
- Dauerhafte Löschung von Daten infolge eines Sicherheitsbruches

Die Rechte der Betroffenen

Die betroffenen Personen, also die Personen deren Daten Sie verarbeiten, haben besondere Rechte:

Informationsrecht

- Auskunfts- und Widerspruchsrecht
- Recht auf Berichtigung, Löschung und Einschränkung
- Recht auf Datenübertragbarkeit

Zum Beispiel kann ein Kunde Sie auffordern, Auskunft darüber zu geben, ob und welche Daten Sie von ihm gespeichert haben.

Datenschutz-Folgenabschätzung DSFA

Als Unternehmen müssen folgende Informationen offengelegt werden:

- Name und Kontaktdaten des Verantwortlichen (ggf. auch des Vertreters)
- Kontaktdaten des Datenschutzbeauftragten (falls vorhanden)
- Zweck und Rechtsgrundlage der Verarbeitung
- Berechtigte Interessen (bei Verarbeitung nach Art. 6 DSGVO)
- Empfänger bzw. Kategorien von Empfängern
- Übermittlung in Drittland oder an internationale Organisation
- Dauer der Speicherung
- Bestehen eines Rechts auf Auskunft, Berichtigung, Löschung, Einschränkung, Widerspruch und auf Datenübertragbarkeit
- Bestehen eines Rechts auf Widerspruch der Einwilligung
- Bestehen eines Beschwerderechts bei einer Aufsichtsbehörde Information,
  ob die Bereitstellung der Daten gesetzlich oder vertraglich vorgeschrieben oder
  für einen Vertragsabschluss erforderlich ist und mögliche Folgen der Nichtbereitstellung

Bestehen einer automatisierten Entscheidungsfindung einschließlich Profiling
Information über eine mögliche Zweckänderung der Datenverarbeitung

Website und Datenschutzerklärung
Wie schon in den vorigen Absätzen erwähnt, ist auch die Website zu beachten.
Neben den Plugins und Cookies die geprüft werden müssen, muss auch die Datenschutzerklärung angepasst werden. Von Generatoren raten wir ab. Warum? Mit einem Generator können Sie keine Rechtssicherheit herstellen. Denn die Datenschutzerklärung muss individuell auf jedes Unternehmen angepasst werden.

Wir helfen Ihnen gerne dabei.

Weitere Informationen

Durch die Einführung der europäischen Datenschutz-Grundverordnung (DSGVO) können Bußgelder in Höhe von 20 Millionen oder 4 Prozent des weltweiten Firmenumsatzes drohen. Zum anderen kann das Unternehmen dank nachweislicher erhöhter Datensicherheit – nicht nur personenbezogene Daten betreffend – das Vertrauen der Kunden und Verbraucher stärken. Der Datenschutz kostet damit nicht nur Geld, sondern kann am Ende auch selbst zur Geldquelle werden.

Wer sich aktiv um Datenschutz kümmert, der minimiert nicht nur das Risiko ein Bußgeld verhängt zu bekommen oder das Vertrauen der Kunden zu verlieren, sondern der gewinnt an Gestaltungsspielraum. Vertrauen ist die beste Technik!

Gerne unterstützen wir Sie und beraten über die möglichen Massnahmen zum Datenschutz in Ihrem Unternehmen.

DAS Labor AG, CH-9427 Wolfhalden
Besuchen Sie uns auf: www.daslaborag.ch

Jasmin Lieffering und **René Rudolf Sonderegger**

Wir halten Datenschutz für ein sehr wichtiges Thema. Durch schlechten Datenschutz werden Unternehmen, egal welcher Größe angreifbar.