HANDELS- UND INDUSTRIEVEREIN
DES KANTONS BERN
Berner Handelskammer

Kramgasse 2, Postfach, 3001 Bern
Telefon 031 388 87 87, Telefax 031 388 87 88
www.bern-cci.ch

DSGVO 2018

Leitfaden zur Umsetzung für die betroffenen Unternehmen

Mit der Unterstützung von:

Inhaltsverzeichnis

1. Übersicht

Die neue europäische Datenschutz-Grundverordnung (DSGVO) verpflichtet alle betroffenen Unternehmen, sich mit geeigneten Instrumenten auszustatten, um die aktuellen Herausforderungen hinsichtlich der Datensicherheit zu bewältigen. Dies kann wesentliche Änderungen in Bezug auf Datenerhebung, -nutzung und -steuerung erforderlich machen.

Dieses neue Konzept der personenbezogenen Daten bevorzugt eine optimierte Gesamtlenkung der Daten und verbessert das Vertrauenskapital des Unternehmens.

Warum sind Schweizer Unternehmen auch betroffen?

Die DSGVO gilt nicht nur für Unternehmen mit Sitz in der Europäischen Union (EU), sie kann auch für Schweizer Unternehmen gelten, auch wenn diese keine Niederlassung oder Tochtergesellschaft in der EU haben.

Der Geltungsbereich der DSGVO umfasst die Datenverarbeitung durch alle Unternehmen, sofern diese Waren oder Dienstleistungen an Personen in der EU anbieten (zum Beispiel: Exporteure, Versandhandel, Betreiber von Online-Bestellplattformen, usw.) oder das Verhalten von Personen analysieren (inklusive auf Webseiten oder Smartphone-Applikationen). Es spielt keine Rolle, ob die Daten in Europa oder in der Schweiz verarbeitet werden.

Ein Vorgeschmack auf die zukünftige Schweizer Gesetzgebung

Gewisse Elemente der neuen europäischen Gesetzgebung werden von der Schweiz im Rahmen des Schengen-Besitzstandes übernommen.

Aus diesem Grund liegt eine Vorlage zur Revision des Bundesgesetzes über den Datenschutz (DSG) bei den eidgenössischen Räten vor.

Diese wird natürlich alle Schweizer Unternehmen betreffen. Die europäische DSGVO bietet die Möglichkeit, sich auf diese zukünftige Entwicklung des Schweizer Rechts vorzubereiten.

Die DSGVO ist auch eine Gelegenheit, um sich abzugrenzen

Der Schutz der Privatsphäre ist - insbesondere nach den Übergriffen, welche von grossen, internationalen Gesellschaften begangen wurden - ein wichtiges Anliegen der Bevölkerung.

Von einem Unternehmen ernst genommen zu werden, ist ein wichtiger Faktor für die Kunden.

Die Grundprinzipien der DSGVO auf einen Blick

Um die Anforderungen der DSGVO zu erfüllen, muss die Verarbeitung personenbezogener Daten durch Ihr Unternehmen folgenden Grundsätzen entsprechen:

Rechtmässigkeit, Fairness, Transparenz	Personenbezogene Daten müssen in Bezug auf die betroffene Person rechtmässig, fair und transparent verarbeitet werden.
Beschränkung der Zweckbindungen	Die Datenverarbeitung muss festgelegten, eindeutigen und rechtmässigen Zweckbindungen dienen, und die Daten dürfen nur für diese konkreten Zwecke verwendet werden.
Datenminimierung	Es dürfen nur die für die (festgelegten) Zwecke erforderlichen Daten verarbeitet werden.
Richtigkeit	Die personenbezogenen Daten müssen korrekt sein. Es müssen alle angemessenen Massnahmen ergriffen werden, um falsche Daten unverzüglich zu löschen oder zu korrigieren.
Begrenzung der Aufbewahrung	Die Aufbewahrungsfristen für personenbezogene Daten dürfen die erforderliche Mindestdauer nicht überschreiten.
Integrität und Vertraulichkeit	Der Schutz personenbezogener Daten muss durch geeignete technische oder organisatorische Massnahmen gewährleistet sein. Dies schliesst den Schutz gegen unbefugte oder rechtswidrige Verarbeitung und den Schutz gegen unbeabsichtigten Verlust, Zerstörung oder Beschädigung mit ein.
Verantwortung	Die für die Datenverarbeitung verantwortliche Person ist für die Einhaltung der genannten Grundsätze verantwortlich und muss nachweisen können, dass diese Grundsätze eingehalten werden. Der/Die Verantwortliche im Sinne der DSGVO ist eine natürliche oder juristische Person, eine Behörde, eine Institution oder ein Dienststelle, welche allein oder kollektiv über die Zweckbindungen der personenbezogenen Daten und über die für die Datenverarbeitung verwendeten Mittel entscheidet.

Rechte der betroffenen Person

Die DSGVO definiert die Rechte, für die durch jede Form der Datenerhebung betroffenen Personen. Die folgende Tabelle fasst die wichtigsten Rechte und Pflichten zusammen, ist aber nicht abschliessend.

Informationspflicht (Art. 13 und 14 DSGVO)	Wenn die Daten erhoben werden, muss die betroffene Person informiert werden. Dies gilt auch, wenn die Daten nicht direkt bei der betroffenen Person erhoben wurden.
Auskunftsrecht (Art. 15 DSGVO)	Die Person hat das Recht, zu wissen, ob ihre personenbezogenen Daten von dem Unternehmen verarbeitet werden oder nicht, und falls ja, um welche Daten es sich hierbei handelt. Dies schliesst die Informationspflicht bei folgenden Elementen ein: die Verarbeitungszwecke, die Datenkategorien, die Kategorien von Empfängern, die Dauer der Aufbewahrung der Daten, das Recht der betroffenen Person auf Berichtigung, Löschung oder Einschränkung der Datenverarbeitung, ein Widerspruchsrecht gegen deren Verarbeitung, ein Beschwerderecht, das Recht, die Herkunft der Daten zu kennen, und gegebenenfalls die Information über das Bestehen einer automatisierten Entscheidung.
Recht auf Berichtigung und Löschung der Daten («Recht auf Vergessenwerden», Art. 16 und 17 DSGVO)	Die betroffene Person hat das Recht, falsche Daten berichtigen zu lassen. Die personenbezogenen Daten müssen, unter anderem, schnellst möglichst gelöscht werden, wenn einer der folgenden Gründe zutrifft: Diese Daten sind für die Zwecke, für die sie erhoben wurden, nicht mehr notwendig; die betroffene Person widerruft ihre Einwilligung, auf die sich die Verarbeitung der Daten stützt und es gibt keine andere Rechtsgrundlage für deren Verarbeitung (z. B. rechtliche Verpflichtung); die betroffene Person widerspricht der Verarbeitung ihrer Daten.
Recht auf Einschränkung der Verarbeitung (Art. 18 DSGVO)	Die betroffene Person hat das Recht, in den gesetzlich bestimmten Fällen von dem/der Verantwortlichen die Einschränkung der Verarbeitung zu verlangen. Wenn eine solche Einschränkung verlangt wurde, hat der/die Verantwortliche für die Verarbeitung nur noch das Recht, diese Daten zu speichern. Grundsätzlich darf in diesem Fall keine weitere Aktion mit diesen personenbezogenen Daten erfolgen.

Mitteilungspflicht des Verantwortlichen (Art. 19 DSGVO)	Dieser Artikel verpflichtet den/die Verantwortliche für die Verarbeitung, die betroffenen Personen über die Berichtigung, Löschung oder Einschränkung der sie betreffenden verarbeiteten Daten zu informieren.
Recht auf Datenübertragbarkeit (Art. 20 DSGVO)	Die betroffene Person kann verlangen, dass der/die Datenverantwortliche ihr die von ihm/ihr übermittelten Daten in einem strukturierten, gängigen und maschinenlesbaren Format zustellt. Das Recht auf Datenübertragbarkeit kann nur unter der Voraussetzung ausgeübt werden, dass die Erstverarbeitung auf einem Antrag auf Einwilligung oder auf einem Vertrag beruht und die Verarbeitung durch ein automatisiertes Verfahren erfolgt.
Widerspruchrecht (Art. 21 DSGVO)	Die betroffene Person hat das Recht gegen die Verarbeitung der sie betreffenden Daten Widerspruch zu erheben. Wenn die betroffene Person der Verarbeitung ihrer Daten widerspricht z. B. für Kundenwerbung, können die personenbezogenen Daten nicht mehr für derartige Zwecke verarbeitet werden.
Das Recht auf Verzicht auf eine automatisierte Entscheidung im Einzelfall (Art. 22 DSGVO)	Die betroffene Person hat das Recht, nicht einer ausschliesslich auf einer automatisierten Verarbeitung beruhenden Entscheidung unterworfen zu werden, die ihr gegenüber rechtliche Wirkung entfaltet oder sie in ähnlicher Weise erheblich beeinträchtigt. Profilierung ist ausdrücklich inbegriffen.
Das Recht auf Benachrichtigung über Datenschutzverletzungen (Art.34 DSGVO)	Der Verantwortliche für die Verarbeitung ist verpflichtet, die betroffene Person über die Verletzung des Schutzes der Daten zu benachrichtigen, die ein hohes Risiko für ihre Rechte und Freiheiten darstellt.

Pflichten des Unternehmens

Die Unternehmen, welche der DSGVO unterliegen, müssen folgenden Pflichten nachkommen:

Informationspflicht	Die Informationen über die Datenerhebung müssen der betroffenen Person in prägnanter, transparenter, verständlicher und leicht zugänglicher Form übergeben werden.
Pflicht zur Durchführung einer Folgenabschätzung (sensible Daten)	Eine Folgenabschätzung zum Datenschutz ist eine Risikoanalyse, die vor der Verarbeitung personenbezogener Daten durchgeführt wird. Sie enthält unter anderem eine Beschreibung der beabsichtigten Verarbeitungsvorgänge, der damit für die betroffene Person verbundenen Risiken und der zu ergreifenden Massnahmen zur Begrenzung oder Minderung der Risiken. Die Folgenabschätzung zum Datenschutz betrifft jedoch nur die Datenverarbeitung, die ein hohes Risiko für die Rechte und Freiheiten der Personen darstellt (z. B. Gesundheitsdaten, die von den Krankenkassen verarbeitet werden, z. B. für Kunden, Benutzer, Mitarbeiter usw.).
Datenschutz durch Technikgestaltung (Privacy by design) und durch datenschutzfreundliche Voreinstellungen (Privacy by default)	Massnahmen müssen getroffen werden, welche das Prinzip des Datenschutzes durch Technikgestaltung (Data Protection by Design) und durch datenschutzfreundliche Voreinstellungen (Data Protection by Default) respektieren. Deshalb muss sichergestellt sein, dass nur die personenbezogenen Daten mit Voreinstellungen verarbeitet werden, die für den spezifischen Zweck der Datenverarbeitung erforderlich sind. Dies gilt für die Menge der erhobenen personenbezogenen Daten, den Umfang ihrer Verarbeitung, ihre Aufbewahrungszeit und ihre Zugänglichkeit.
Dokumentationspflicht	Die Verantwortlichen für die Datenverarbeitung müssen über ihre Verarbeitungstätigkeiten ein (schriftliches oder elektronisches) Verzeichnis führen. Dieses Verzeichnis muss unter anderem die folgenden Angaben enthalten: Namen und Kontaktdaten des oder der Verantwortlichen für die Datenverarbeitung und seines/ihres Vertreters sowie eines eventuellen Datenschutzbeauftragten; die Zwecke der Verarbeitung; die Beschreibung der Kategorien betroffener Personen und die Kategorien personenbezogener Daten (z. B. Kunden und Lieferanten; Rechnungsdaten, Kontaktdaten); die Kategorien von Empfängern, welchen die personenbezogenen Daten mitgeteilt wurden oder werden (z. B. Polizei, Sozialversicherungen), einschliesslich Empfängern in Drittländern oder internationalen Organisationen (Muttergesellschaft in den Vereinigten Staaten); sofern möglich, die für die Löschung der verschiedenen Datenkategorien vorgesehenen Fristen, wenn möglich, eine allgemeine Beschreibung der technischen und organisatorischen Sicherheitsmassnahmen für den Datenschutz.

Definition von «personenbezogene Daten»

Personenbezogene Daten betreffen alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen, zum Beispiel Name, Vorname, Adresse, Geburtsdatum, Telefonnummer, E-Mail-Adresse, Zahlungsmittel usw.

Definition von «sensiblen personenbezogene Daten»

Sensible personenbezogene Daten geben, direkt oder indirekt, Informationen bekannt im Zusammenhang mit: der Gesundheit; der Intimsphäre oder rassische oder ethnische Herkunft; Sozialhilfemassnahmen; religiöse, philosophische, politische oder gewerkschaftliche Meinungen oder Aktivitäten; Straf- oder Verwaltungsverfahren oder Sanktionen; biometrische und genetische Daten, usw.

Definition des Data Protection Officer (DPO) oder «Verantwortlicher für die Verarbeitung»

Der DPO oder «Verantwortlicher für die Verarbeitung» ist rechtlich dafür verantwortlich, dass die Regeln der DSGVO – beziehungsweise des Schweizer DSG – vom Unternehmen eingehalten werden. Es liegt ihm zu, die technischen Lösungen umzusetzen, die für die Einhaltung der Gesetzgebung notwendig sind. Er ist es auch, der im Falle eines Verstosses gegen die geltenden Normen als Gesprächspartner mit den Behörden dient.

Diese Funktion kann nicht von der Geschäftsleitung des Unternehmens übernommen werden. Sie kann entweder einem Mitarbeiter, einem Verwalter oder einer Drittperson ausserhalb des Unternehmens übertragen werden.

Bis heute, gibt es noch keine spezifische Ausbildung für die Funktion des DPO, die an die Bedürfnisse einer KMU angepasst sind. Allerdings sind umfassende Kenntnisse der Gesetzgebung unerlässlich.

2. Geist des Gesetzes und Identifizierung der Risiken

Es liegt an den Unternehmen, die Risiken einzuschätzen und die geeigneten Massnahmen zu ergreifen in Bezug auf die Konformität und die Anwendung des Gesetzes. Datenschutz und rigorose Dokumentation bleiben von grundlegender Bedeutung. Die Unterstützung, wie sie in einem Qualitätsmanagementsystem erfolgt, muss jederzeit die Konformität der DSGVO zu beweisen können und dies in der Logik der Unternehmensverantwortung.

In diesem Sinne müssen diese das **Verarbeitungsverzeichnis** und alle anderen Dokumente, die ihre Konformität beweisen, auf dem neuesten Stand halten (Verzeichnis des PIA/Privacy Impact Assessment, dokumentierte Sicherheitspolitik, interne Verfahren, Einwilligungsbeweis usw.)

Die DSGVO definiert eine Reihe von **Grundsätzen** zum Schutz der personenbezogenen Daten. Die Unternehmen müssen, je nach ihrer Situation und ihrem Kontext, die geeigneten Mittel festlegen, um diesen zu entsprechen, und **dies während des gesamten Datenlebenszyklus; Speicherung, Aufbewahrung, Zugänglichkeit, Einsichtsrechte...**

Die Verantwortlichkeiten werden auch auf Subunternehmer ausgedehnt. Die Dienstleister, die personenbezogene Daten im Auftrag des Unternehmens verarbeiten, müssen selbst die DSGVO einhalten und haben Verpflichtungen zur Vertraulichkeit und Datensicherheit. Sie können das Unternehmen auch im Falle einer Sicherheitsverletzung, Datenvernichtung usw. beraten.

- ✓ **Rechtliches Risiko: die fehlende Konformität der DSGVO kann schweren Sanktionen unterliegen.** Diese reichen von einer Pauschalgeldbusse bis hin zu einer Geldbusse, die einen Prozentsatz des Umsatzes des Unternehmens ausmacht. Über der Geldbusse hinaus, ist das Unternehmen verpflichtet, die notwendigen Massnahmen für die Einhaltung der Konformität, Mittelbeschaffung inklusive, zu ergreifen.

- ✓ **Sicherheitsrisiko:** Mit der DSGVO ist die Datensicherheit nicht mehr eine Option, sondern ein Teil der einzuhaltenden Standards. **Die Investition in eine Datensicherheitspolitik wird unerlässlich,** um sowohl das Rechtsrisiko, **die Versicherungsprämien** (Die Praxis von Sicherheitsprüfungen durch Versicherungsgesellschaften wird gängig, bevor die Höhe der Prämie festgelegt wird), als auch die durch einen Cyberangriff verursachten Kosten (Datenverlust, Geschäftsverlust, Reputationsverlust...) zu begrenzen.

- ✓ **Reputationsrisiko:** Es ist mit der Datensicherheit verbunden, denn je nach Fall des Angriffs oder der Verletzung der personenbezogenen Daten, müssen die Unternehmen die betroffenen Personen, sowie die Aufsichtsbehörde innerhalb von 72 Stunden informieren. Sobald ein Unternehmen gehackt wird, verbreitet sich die Nachricht sehr schnell und sein Ruf wird zwangsläufig beschädigt. Obwohl es schwierig ist, die finanziellen Auswirkungen im Zusammenhang mit der Reputation des Unternehmens genau zu messen, zeigt der Breach Level Index von Gemalto trotzdem, dass zwei Drittel der Unternehmen, welche Opfer von Sicherheitslücken waren, vom Kurs der börsenkotierten Aktien beeinflusst wurden.

- ✓ **Finanzielles Risiko:** Die Sanktionen für Grossunternehmen können zu einer Geldbusse in Höhe von bis zu 20 Millionen Euro oder **4 % des gesamten weltweit erzielten Jahresumsatzes** führen.

3. Gebiete und Anwendungsbereiche des Gesetzes

Eine Verpflichtung zur Gewährleistung der Sicherheit der verarbeiteten Daten

Eine Charakterisierung der verschiedenen Datentypologien, wie z. B. sensible, strategische, veraltete oder redundante Daten, muss durchgeführt werden. Diese erste Phase ermöglicht, die Datenbanken zu bereinigen und die Speicherkosten zu senken (Welche Daten sind gespeichert? Wie wurden die Daten erhalten? Sind sie aktuell? Wofür werden sie verwendet? usw.). Viele KMU verfügen über mehrere Datenbanken, die nicht oder schlecht gepflegt wurden, oft unzureichend benutzt und so fragmentiert sind, dass diese nicht mehr wissen, woher die Daten stammen.

Um dies zu beheben, müssen Sie:

- die Relevanz der Verarbeitungspolitik überprüfen: Erfassung, Änderung, Extraktion, Speicherung, Vernichtung der Daten im Unternehmen.
- Ihre Mitarbeiter, welche die Daten der Kunden verarbeiten, einer Geheim-haltungspflicht unterziehen.
- Ihren Kunden jegliche Verletzung seiner Daten mitteilen.
- alle Massnahmen ergreifen, um ein den Risiken angemessenes Schutzniveau zu gewährleisten. Zu diesem Zweck ist eine umfassende Zählung zur Beurteilung der Relevanz der Daten im Hinblick auf die Entwicklungsschwerpunkte erforderlich.

Das Recht auf Einwilligung von Personen wird gestärkt

Bei jeder Erfassung von personenbezogenen Daten müssen die Benutzer die Möglichkeit haben, eine **ausdrückliche Einwilligung** zu erteilen oder abzulehnen. Es reicht nicht mehr, eine allgemeine Datenschutzpolitik zu akzeptieren. Der Benutzer muss verstehen, welche Daten erhoben werden, zu **welchem Zweck**, wie lange **sie aufbewahrt werden** und welche Folgen eine Einwilligung oder Ablehnung für den Benutzer hat. Es liegt am Unternehmen, bei jeder Datenerhebung klare und verständliche Informationserklärungen zu erfassen und den Nachweis der Einwilligung der Personen zu wahren.

Die betroffenen Personen müssen informiert werden, dass sie jederzeit auf ihre personenbezogene Daten Zugriff haben, diese löschen oder übertragen lassen können. Dies erfolgt durch die Änderung Ihrer Verträge, Haftungsausschuss auf der Webseite (Disclaimers), usw.

- ✓ **Recht auf Vergessenwerden:** Das Unternehmen muss auf einfachen Wunsch auch in der Lage sein, einen Kunden auszulisten. Die Problematik der **Aufbewahrungsfrist** der Daten betrifft auch die Aufbewahrung der Daten der Mitarbeiter, die das Unternehmen verlassen haben. Achten Sie jedoch auf die Einhaltung der schweizerischen Verordnung über die Führung und Aufbewahrung der Geschäftsbücher (GeBüV), welche die Daten und Aufbewahrungsfristen definiert, die trotz eines Löschungsauftrags einer betroffenen Person zu berücksichtigen sind.

- ✓ **Benachrichtigung bei Datenschutzverstoss:** Innerhalb von 72 Stunden nach einem Datenschutzverstoss muss das Unternehmen die betroffenen Personen und die zuständigen Aufsichtsbehörden informieren. Achtung, dies ist nur dann geltend, wenn ein Schweizer Unternehmen der DSGVO unterworfen ist und einen Vertreter innerhalb der EU genannt hat.

- ✓ **Betreuung der Übertragung der Daten ausserhalb der Schweiz:** Die Daten-übertragungen ausserhalb der Schweiz sind nur möglich, wenn sie mit Mitteln überwacht werden, die eine auszureichende und angemessene Schutzstufe gewährleisten. Dies gilt auch für die personenbezogenen Daten, die auf «**cloud**» gespeichert sind. **Das Gesetz gewährleistet die Integrität und den Schutz dieser Daten in allen Umgebungen.**

- ✓ **Sicherheit und Dokumentation:** Die Datensicherheitspolitik ist ein wichtiger Aspekt bei der Einhaltung der DSGVO. Das Unternehmen muss die notwendigen **organisatorischen und technischen** Massnahmen ergreifen, so dass die personenbezogenen Daten, die sie verwaltet, von der höchsten Sicherheitsstufe profitieren. Diese muss natürlich **an die Risiken und die Sensitivität der Daten** angepasst sein. Es geht auch darum, die Integrität des Informationssystems, seine Verfügbarkeit und seine **Widerstandsfähigkeit im Falle eines Vorfalls** zu gewährleisten.

Eine Information muss auf das Verarbeitungsverzeichnis aufgeführt sein zwecks **besserer Rückverfolgbarkeit,** was auch die Abfassung von Vermerken der Informationen erleichtert.

Orte identifizieren, wo die Daten aufbewahrt werden, sowie die möglichen Risiken von Übermittlungen ausserhalb der Schweiz.

Die Identifizierung der Personen, die die Daten verarbeiten, und gegebenenfalls die externen Agenten, welche an jeder Verarbeitung beteiligt sind, trägt zur Rückverfolgbarkeit der Daten bei.

Interne Verfahren: Legen Sie einen Rahmen für die Gewährleistung dieses Schutzes fest, indem Sie klare Richtlinien und Rundschreiben zuhanden der betroffenen Akteure erlassen.

Konformität Ihrer zukünftigen Marketingaktionen gewährleisten: Jede neue Marketingaktion so vorbereiten, dass der Respekt der Rechte der Personen und die Datensicherheit von Anfang an gewährleistet wird.

Viele Marketingpraktiken basieren auf dem Konzept der Profilierung, d. h. der Erhebung von personenbezogenen Daten, mit dem Ziel, ein Profil Ihrer potenziellen Kunden, existierenden Kunden oder Benutzer zu erstellen, um ihnen personalisierte Angebote oder Dienstleistungen anzubieten.

Die Profilierung zu Marketingzwecken ist erlaubt, solange sie die Bedingungen der DSGVO erfüllt (die Person muss darüber informiert sein und muss Widerspruch erheben können).

Opt-in (Beitrittsoption) verstärkt und Cookie-Management: Die verstärkte Informationspflicht zugunsten der Internetbenutzer bedeutet, dass er freiwillig seine Einwilligung zu perfekt identifizierten Verarbeitungen erteilen kann (Art und Zweck der Erhebung müssen genau angegeben werden).

Abgesehen von Ausnahmen, muss der Internetbenutzer seine vorherige Einwilligung für die Hinterlegung eines Cookies geben. Folglich muss ein Informationsbanner auf allen Webseiten vorhanden sein.

DATENERHEBUNG	DATENBEWERTUNG
Nun ist es notwendig, den Kunden genau über die **die Verwendung der Daten,** welche von ihm erzeugt werden, zu informieren.	Falls Sie beabsichtigen, die personenbezogene Daten in Ihren Marketingkampagnen zu verwenden, ist es notwendig, **vorher die Einwilligung des Kunden einzuholen und ihm erlauben, diese abzulehnen.**
Das Unternehmen muss die Einwilligung des Kunden in **klarer und sachkundiger Weise** einholen (die Bedingungen für die Verwendung seiner Daten zur Verfügung stellen).	Beim Austausch seiner Daten, sollte der Kunde angeben können, ob er von diesen **Marketingkampagnen angesprochen werden** möchte oder nicht.
Eine Einwilligung nach Aufklärung ist ein zentrales Konzept der DSGVO: Der Kunde muss nun immer eine **erweiterte Wahrnehmung** der Absichten des Unternehmens haben.	Der Kunde kann auch **seine Profilerstellung ablehnen**, d.h., dass seine Daten über einen Algorithmus für Marketing- und kommerzielle Zwecke verwendet werden könnten.

4. Vorbereitung: Verfügbare Methoden und Instrumente

Mapping der Datenverarbeitung

Der erste Schritt besteht darin, ein Verzeichnis aller Verarbeitungen des Unternehmens von personenbezogenen Daten zu erstellen.

- Die verschiedenen Verarbeitungen von personenbezogenen Daten.
- **Die Kategorien von verarbeiteten personenbezogenen Daten**, nach Grad der Sensibilität.
- **Die verfolgten Ziele** der Datenverarbeitung.
- **Die Akteure** (intern oder extern), die diese Daten verarbeiten; Sie werden insbesondere die Subunternehmer eindeutig identifizieren müssen.
- **Die Dateneinspeisung** unter Angabe von Herkunft und Bestimmungsort der Daten, um mögliche **Datentransfers ausserhalb der Schweiz** zu identifizieren und eine zuverlässige **Rückverfolgbarkeit** zu gewährleisten

Im Rahmen einer zukünftigen Verordnung, müssen die Stellen eine **vollständige interne Dokumentation** über ihre Verarbeitungen der personenbezogenen Daten führen und sicherstellen, dass sie die neuen gesetzlichen Verpflichtungen einhalten.

Für jede Verarbeitung personenbezogener Daten, stellen Sie sich folgende Fragen:

WER?	✓ Tragen Sie in das Verzeichnis den Namen und die Kontaktdaten des **Verantwortlichen für die Verarbeitung** (operative Dienste), gegebenenfalls des **Datenschutz-beauftragten**. ✓ Erstellen Sie eine Liste der **Subunternehmen**.
WAS?	✓ Identifizieren Sie die Kategorien der verarbeiteten Daten. ✓ Identifizieren Sie die Daten, die aufgrund ihrer besonderen **Sensibilität** Risiken bergen können (zum Beispiel: Gesundheitsdaten oder Straftaten).
WARUM?	✓ Identifizieren Sie den Zweck oder die Zwecke, für die Sie diese Daten erheben oder verarbeiten (zum Beispiel: Verwaltung der Geschäftsbeziehungen, HR-Management...).
WO?	✓ Bestimmen Sie, wo die Daten gespeichert werden. ✓ Geben Sie an, in welche Länder die Daten eventuell übertragen werden.
BIS WANN?	✓ Geben Sie für jede Datenkategorie an, wie lange Sie diese aufbewahren (Archivierung der Daten und ungerechtfertigte Speicherung ausserhalb der zulässigen offiziellen Fristen).
WIE?	Geben Sie die Sicherheitsmassnahmen genau an, die umgesetzt werden, um das **Risiko eines unbefugten Zugriffs auf Daten** und somit die Auswirkungen auf die Privatsphäre zu minimieren.

Datenverwaltung und -übertragung

Von jetzt an kann das Unternehmen die Daten nicht mehr auf unbestimmte Zeit speichern. Die Dauer muss an den Zweck gebunden sein. Ausserdem müssen die Verantwortlichen der Datenverarbeitung ein detailliertes Verzeichnis der Verarbeitungen bewahren.

Die Übertragung der personenbezogenen Daten in Ländern ausserhalb der EU unterliegt einer Überprüfung. Bei der Übertragung von Daten an andere Unternehmen sind eine Anonymisierung und Verschlüsselung der Daten zwingend erforderlich. Schliesslich sollten nur autorisierte Personen Zugang auf die Daten haben. Dies schützt nicht nur die Benutzer, sondern auch Ihre Datenbanken!

Sie haben diesen Schritt abgeschlossen, wenn

- ✓ **Sie die Dienste und Einrichtungen, die die personenbezogenen Daten verarbeiten, kennengelernt haben. Sie haben die Liste der Verarbeitungen nach Hauptzweckbindung und Sensibilisierung erstellt.**
- ✓ **Sie die an diesem Prozess beteiligten Subunternehmer identifiziert haben.**
- ✓ **Sie wissen, wo diese Daten gespeichert sind, wer darauf Zugriff hat und wie lange.**

Priorisierung der auszuführenden Aktionen

Auf der Grundlage des Verarbeitungsverzeichnisses von personenbezogenen Daten, identifizieren Sie die Massnahmen, die zu ergreifen sind, um aktuelle und zukünftigen Verpflichtungen nachzukommen.

Diese Massnahmen angesichts der Risiken, die Ihre Verarbeitung für die Rechte und Freiheiten der betroffenen Personen mit sich bringt, sind vorrangig zu behandeln.

- Falls erforderlich, überprüfen und überarbeiten Sie die Vertragsklauseln **mit Subunternehmer**.
- Verfahren zur Ausübung der Rechte der Person einplanen (Recht auf Datenübertragbarkeit usw.)
- Überprüfung der **aktuellen Sicherheitsstufe** der laufenden Verarbeitungen

Nachdem Sie die in Ihrer Organisation umzusetzenden Datenverarbeitungsvorgänge identifiziert haben, müssen Sie für jeden von ihnen die Massnahmen festlegen, die zu ergreifen sind, um den gegenwärtigen und zukünftigen Verpflichtungen nachzukommen.
Zu beachtende Punkte, unabhängig von den Datenverarbeitungen:

- **Stellen Sie sicher,** dass nur Daten erhoben und verarbeitet werden, die für die Erreichung Ihrer Ziele **unbedingt erforderlich** sind.
- **Identifizieren Sie die Rechtsgrundlage**, auf die Ihre Verarbeitung beruht (zum Beispiel: Einwilligung der Person, berechtigtes Interesse, Vertrag, rechtliche Verpflichtung).
- **Überprüfen** Sie Ihre Informationshinweise, so dass diese den Anforderungen der Verordnung **entsprechen**.

- **Überprüfen** Sie, ob sich Ihre Subunternehmer ihrer neuen Verpflichtungen und Verantwortlichkeiten bewusst sind. Stellen Sie sicher, dass es Vertragsklauseln gibt, die sie an die Verpflichtungen des Subunternehmers hinsichtlich Sicherheit, Vertraulichkeit und Schutz der verarbeiteten personenbezogenen Daten erinnern.

- **Planen Sie** die Modalitäten der Ausführung der Rechte der betroffenen Person (Recht auf Zugang, Berichtigungsrecht, Recht auf Datenübertagbarkeit, Widerruf der Einwilligung...).

- **Überprüfen** Sie die eingerichteten Sicherheitsmassnahmen.

Fokuspunkte, die besondere Aufmerksamkeit erfordern

Zusätzlich zu den im vorherigen Absatz genannten Punkten, bedürfen die in der folgenden Tabelle genannten Fälle besonderer Aufmerksamkeit!

Sie verarbeiten bestimmte Arten von Daten	• Daten aus denen die angebliche rassische und ethnische Herkunft hervorgeht. • Politische, philosophische oder religiöse Meinungen, Gewerkschaftszugehörigkeit. • Daten bezüglich Gesundheit oder sexuelle Orientierung. • Genetische oder biometrische Daten. • Daten über Straftaten oder strafrechtliche Verurteilungen. • Daten bezüglich Minderjähriger.
Ihre Verarbeitung von personenbezogenen Daten hat zur Folge	• Systematische grossräumige Überwachung eines öffentlich zugänglichen Bereichs. • Die systematische und gründliche Auswertung persönlicher Aspekte, einschliesslich der Erstellung von Profilen, auf deren Grundlage Sie Entscheidungen treffen, die Rechtswirkungen auf eine natürliche Person haben oder diese erheblich beeinträchtigen.
Übertragen Sie Daten ausserhalb der Schweiz?	• Überprüfen Sie, ob das Land, in das Sie die Daten übertragen, von den Aufsichtsbehörden als angemessen anerkannt wird. • Ist dies nicht der Fall, überwachen Sie Ihre Übertragungen.

Sie haben diesen Schritt abgeschlossen, wenn:

- ✓ ***Sie die ersten Massnahmen zum Schutz der von Ihren Verarbeitungen betroffenen Personen getroffen haben.***

5. Verwaltung, Identifikation und Minimierung der Risiken

Wenn Sie Datenverarbeitungen identifiziert haben, durch die ein hohes Risiko für die Rechte und Freiheiten der betroffenen Personen entstehen kann, müssen Sie für jeden dieser Verarbeitungen eine Folgenabschätzung zum Datenschutz durchführen (Englisch: **Privacy Impact Assessment oder PIA**).

Es ist ein unverzichtbares Instrument, das Ihnen ermöglicht zukünftige Risiken zu minimieren und Verstösse gegen die vorgelagerten Daten zu verhindern.

Diese Abschätzung oder diese Revision besteht aus:

- Identifizierung der Art der eingegangenen Risiken für das Privatleben ab Entwurf eines neuen Produkts oder einer neuen Dienstleistung, d.h. eine Auswertung der Relevanz und Verhältnismässigkeit des Verarbeitungsvorgangs in Bezug auf das Risiko.

- Bestimmung der Art der Verarbeitung der personenbezogenen Daten und dessen Zweckbindung.

- Bestandsaufnahme der eingerichteten Mittel zur Sicherung der Verarbeitung und Gewährleistung der Vertraulichkeit der Daten.

- Bestätigung der Lösungen (technisch und organisatorisch) zur Minimierung der mit der Verarbeitung verbundenen Risiken.

Die Folgenabschätzung bezüglich Datenschutzes ermöglicht es:

- eine Verarbeitung der personenbezogenen Daten oder ein datenschutzfreundliches Produkt **einzurichten**.

- die Auswirkungen auf das Privatleben der betroffenen Personen **auszuwerten**.

- **aufzuzeigen**, dass die Grundprinzipien der Verordnung eingehalten werden.

Die Instrumente, die Ihnen helfen können:

- **zu schützende Elemente**: Minimierung der Daten, Verschlüsselungen, Anonymisierungen (Anonymus), Ausübung von Rechten ermöglichen usw.

- **Mögliche Auswirkungen**: Daten sichern, Aktivität verfolgen, Datenverletzungen verwalten usw.

- **Risikoquellen**: Zugang kontrollieren, Verwaltung von Dritten, Bekämpfung von bösartigen Codes usw.

- **Supports**: Schwachstellen bei Hardware, Software, Netzwerken und Papierdokumenten reduzieren usw.

Sie haben diesen Schritt abgeschlossen, wenn*:*

✓ ***Sie Massnahmen ergriffen haben, um die wichtigsten Risiken und Bedrohungen für das Privatleben der betroffenen Personen zu beseitigen.***

Reorganisation des internen Prozesses

Um ständig einen hohen Schutzgrad der personenbezogenen Daten zu gewährleisten, richten Sie interne Verfahren und Praktiken ein, um den Datenschutz jederzeit zu gewährleisten, wobei alle Ereignisse zu berücksichtigen sind, die während der Lebensdauer einer Verarbeitung von personenbezogenen Daten auftreten können (zum Bespiel: Sicherheitslücken, Verwaltung von Berechtigungs- oder Zugriffsanfragen, Änderung der erfassten Daten, Dienstleisterwechsel usw.).

Auswirkungen des Prozessorganisation

- **Berücksichtigen** Sie den Schutz der personenbezogenen Daten **bei der Gestaltung** einer Anmeldung oder Verarbeitung.

- **Sicherstellung** der Rolle und Verantwortung der an der Umsetzung der Datenverarbeitung beteiligten Akteure, **Sensibilisierung und Organisation** des Feedbacks durch Erstellung eines **Ausbildungs- und Kommunikationsplans** der Mitarbeiter.

- Jeder Mitarbeiter, der mit sensiblen Daten umgehen kann, muss sich der bewährten Verfahren bewusst sein, um deren Schutz und Vertraulichkeit zu gewährleisten.

- **Bearbeitung von Beschwerden** und Anfragen der betroffenen Personen über die Ausübung ihrer Rechte **(Zugangsrechte, Berichtigung, Widerspruch, Recht auf Datenübertragbarkeit, Widerruf der Einwilligung)** durch Festlegung der Akteure und Verfahren (die Ausübung der Rechte muss auf elektronischem Wege möglich sein, wenn die Daten auf diesem Wege erhoben wurden).

- **Antizipieren** Sie Datenschutzverletzungen, indem Sie in bestimmten Fällen innerhalb von 72 Stunden der Datenschutzbehörde und so schnell wie möglich den Aufsichtsbehörden und betroffenen Personen Meldung erstatten.

Sie haben diesen Schritt abgeschlossen, wenn*:*

✓ ***Datenschutzreflexe innerhalb der Dienste, die Datenverarbeitungsvorgänge durchführen, erfasst und angewendet werden; Ihre Organisation weiss, was zu tun ist und an wen sie sich im Falle eines Vorfalls wenden muss.***

6. Seine Konformität gut dokumentieren

Ihr Unternehmen hat einen langen Weg zurückgelegt, um die **Konformität** bezüglich der neuen europäischen Verordnung zu **gewährleisten**. Um seine Konformität nachzuweisen, müssen Sie **verschiedene Dokumente vorlegen, die regelmäßig aktualisiert werden müssen.**

Diese Überarbeitung muss einen kontinuierlichen Datenschutz gewährleisten.

- Verzeichnis der vollständig erfassten Verarbeitungen erstellen
- Folgenabschätzung an allen Hochrisikoverarbeitungen durchführen
- Informationshinweise überarbeiten
- Verfahren zur Einholung der Einwilligung und Ausübung von Benutzerrechten einrichten
- Vertragsklauseln mit Subunternehmer überarbeiten

Um Ihre Konformität nachzuweisen, müssen Sie eine Dokumentation erstellen, die nachweist, dass die Verarbeitung personenbezogener Daten den Vorschriften entspricht. Die organisatorischen und technischen Massnahmen werden noch einmal überprüft und bei Bedarf aktualisiert.

Ihre Akte muss insbesondere folgende Elemente beinhalten

Zum einen die Dokumentation zu Ihren Verarbeitungen von personenbezogenen Daten (Name und Vorname, Passwörter, Geburtsdatum usw.)

- **Das Verzeichnis der Verarbeitungen** (für die Verantwortlichen der Verarbeitungen) oder die Kategorien der Verarbeitungsaktivitäten (für die Subunternehmer).
- **Die Folgenabschätzungen bezüglich Datenschutzes** (siehe Kapitel 4 «Vorbereitung: Verfügbare Methoden und Instrumente») für die Verarbeitungen, die ein hohes Risiko für die Rechte und Freiheiten der Personen darstellen können, Betreuung der Übertragung der Daten ausserhalb der Schweiz.

Andererseits werden die Informationen an Personen innerhalb und ausserhalb des Unternehmens weitergegeben (Mitarbeiter, Kunden, Lieferanten usw.).

- Die Informationshinweise
- Die Vorlagen zur Einholung der **Einwilligung** der betroffenen Personen
- **Die eingerichteten Verfahren** für die Ausübung der Rechte der Personen
- Die internen Verfahren im Falle von **Datenschutzverletzungen**

7. Fragebogen und konkrete technische Massnamen

- Bereiten Sie sich auf die Möglichkeit eines Datenverlustes vor: Einrichtung von Eskalationsverfahren, die bei einer Verletzung der personenbezogenen Daten aktiviert werden.

- Informieren Sie die Internetbenutzer, die auf Ihre Webseite zugreifen, über ihre Rechte (*Löschung, Datenübertragbarkeit*)?

- Sind die Pflichtfelder Ihrer Formulare mit einem Sternchen gekennzeichnet?

- Stimmen Internetbenutzer dem Erhalt von Cookies zu, wenn sie Ihre Webseite besuchen?

- Ist die Aufbewahrungsdauer für die von Ihnen gesammelten Daten unbegrenzt?

- Haben Sie die von Ihnen durchgeführten Datenverarbeitungsvorgänge aufgelistet?

- Alle anderen organisatorischen und technischen Vorkehrungen.

Notwendigkeit alle Daten in Bezug auf Vertraulichkeit und Sicherheit gleich zu behandeln

- Wurde ein Opt-in-System (Opt-in-Option) für den E-Mail-Verkehr (z.B. Newsletter) eingerichtet?

- Werden Daten, die ausserhalb der Schweiz erhoben werden (Tochtergesellschaften, Partner, Server usw.), übertragen?

- Notwendigkeit die gesammelten personenbezogene Daten zu dokumentieren, ihre Herkunft und wer sie erhält.

- Notwendigkeit bestehende Datenschutzerklärungen zu überprüfen und gegebenenfalls Änderungen vorzunehmen.

- Notwendigkeit einer Überprüfung der Verfahren, um die neuen Rechte natürlicher Personen zu wahren.

- Notwendigkeit die Art von Bearbeitung von Anträgen zu planen, unter Achtung der neuen Fristen und die gewünschten Informationen vorlegen.

- Notwendigkeit, Rechtsgrundsätze für jede Art von Datenverarbeitungstätigkeit zu ermitteln und zu dokumentieren.

- Notwendigkeit sicherzustellen, dass angemessene Verfahren zur Erkennung, Meldung und Untersuchung von Datenschutzverletzungen eingerichtet wurden.

Sichere Speicherung und Übermittlung der sensiblen Informationen

- Segmentieren Sie das Netzwerk und überwachen Sie, wer es betritt und verlässt, stellen Sie Verarbeitungsverzeichnisse (Dokumente/Entlassungsformulare) zur Verfügung.

- Sichern Sie Papierdokumente, physische Medien und Geräte.

- Sicherstellen, dass wichtige Abteilungen über die regulatorische Änderung informiert werden und die Auswirkungen der DSGVO vorwegnehmen.

- Verfahren zur Aufrechterhaltung der Sicherheit und zur **Behebung von Schwachstellen** haben.

Fernzugriff sichern

- Sicherstellen, dass Anbieter von **externen Dienstleistungen** Sicherheitsmassnahmen einrichten.

Verwaltung der Zugriffe – Eine solide Identitäts- und Zugriffsverwaltung umfasst Authentifizierung, sicheren Fernzugriff, adaptive/risikobasierte Sicherheit, Passwortverwaltung und Benutzeridentifikationskontrolle. Für den Zugriff auf sensible Daten empfiehlt der Gesetzgeber eine Authentifizierung mit erhöhter Sicherheit (z. B. mit sicheren Passwörtern von 12 alphanumerischen Zeichen, darunter mindestens ein Sonderzeichen, das regelmässig geändert wird).

Schutz des Perimeters – Setzen Sie Firewalls der nächsten Generation (NGFW) ein, um die Gefährdung des Netzwerks durch Cyber-Bedrohungen zu verringern, das Risiko eines Lecks zu vermeiden und geeignete Korrekturmassnahmen nach einem Verstoss zu ergreifen.

Sichere mobile Zugriffe – Die betreffenden Daten müssen absolut sicher zirkulieren können und die Mitarbeiter müssen über die Terminals ihrer Wahl auf die von ihnen benötigten Anwendungen und Daten nach eigenem Ermessen zugreifen können.

Schutz der E-Mails – Phishing-Bedrohungen und andere Angriffe auf E-Mail-geschützte Informationen verhindern und gleichzeitig den sicheren und konformen Austausch vertraulicher Daten gewährleisten.

Sensibilisieren Sie alle Mitarbeiter – Die Aufmerksamkeit der letzteren auf Datenlecks zu lenken und auf die Notwendigkeit, ihre Verarbeitung zu sichern, gegebenenfalls Schulungen anbieten: Falls die Hackerprobleme Schlagzeilen machen, Datenlecks können viel alltäglichere und weniger spektakuläre Formen annehmen: Diebstahl eines professionellen Computers, Versand eines Anhangs mit Daten eines anderen Kunden usw.

Überprüfung der Art und Weise, wie die Einwilligung angefragt, eingeholt und aufbewahrt werden.

8. Schlussfolgerung

Viele Schweizer Unternehmen haben bereits die notwendigen Anpassungen vorgenommen. Zu den vorrangigen Massnahmen gehören unter anderem:

- **Ernennung:** einen Datenschutzbeauftragten (DPO) ernennen, der sicherstellt, dass die Datenverarbeitung den Anforderungen entspricht.
- **Bestandsaufnahme:** ein Datenverarbeitungsverzeichnis führen.
- **Identifizierung:** den Umfang der sensiblen Daten identifizieren. Die DSGVO verlangt für diese Daten eine Verschlüsselung oder Pseudonymisierung.
- **Recht der Personen gewährleisten**: Recht auf Vergessenwerden, Recht auf Datenübertragbarkeit usw.
- **Ausbildung:** eine Charta bewährter Praktiken für die Mitarbeiter zu erstellen, einschließlich Sanktionen bei Nichteinhaltung des Gesetzes.
- **Anpassung:** Klauseln in die Verträge Ihrer Subunternehmer und Mitarbeiter einfügen, die garantieren, dass sie die gesetzlichen Bestimmungen über die Daten, die sie Ihnen anvertrauen, einhalten.
- **Validierung:** Anpassung von Software und Anwendungen zur Sicherstellung der Einhaltung der neuen Regeln und Normen der DSGVO und ISO.
- **Verwaltung:** Vorbereitung auf die Möglichkeit eines Datenlecks. Zu diesem Zweck implementieren Sie die Eskalationsverfahren, die im Falle eines Verstosses gegen personenbezogene Daten aktiviert werden.
- **Schutz:** Verwaltung der Zugriffsrechte auf personenbezogene Daten und Internetzugriffe.

Weitere Informationen

- Synthese auf einer Seite www.bern-cci.ch
- Test zur Selbstdiagnose online www-bern-cci.ch

Kontakte und nützliche Adressen

- Handels- und Industrieverein des Kantons Bern www.bern-cci.ch
- IGESCO Schweiz AG, IT-Spezialist für KMU, www.igesco.ch
- Kellerhals Carrard, Anwaltskanzlei, www.kellerhals-carrard.ch
- Swisscom Solutions PME, www.swisscom.com
- Credit Suisse, www.credit-suisse.com
- Mazars Suisse, Treuhänder und Wirtschaftsprüfung, www.mazars.ch
- GestConseil AG, Versicherungsberater und Makler, www.gestconseil.ch
- De la Cruz & Beranek Rechtsanwälte, www.delacruzberanek.com
- Datenschutz- und Öffentlichkeitsbeauftragter des Kantons Wallis, www.prepose.tv

Disclaimer

Das vorliegende Informationsblatt und das Online-Test dienen nur zu Informations- und Sensibilisierungszwecken. Sie können eine Rechtsberatung nicht ersetzen. Der Handels- und Industrieverein des Kantons Bern und seine Partner lehnen jede Verantwortung im Falle von Handlungen oder Unterlassungen im Zusammenhang mit der Einsicht des Informationsblattes und der Nutzung des Online-Tests.

Impressum

Handels- und Industrieverein des Kantons Bern
Walliser Industrie- und Handelskammer

Bern, April 2019