Hinweise zum Datenschutz für Zuschussempfänger im Rahmen von Projekten aus den Bereichen Erasmus+ und Europäisches Solidaritätskorps

Im Prinzip wird der rechtliche Rahmen zum einen durch die Datenschutzgrundverordnung, kurz DSGVO, und zum anderen durch den Vertrag mit der Nationalen Agentur definiert. Daraus leiten sich alle Rechte und Pflichten ab.

Es kann jedoch im konkreten Anwendungsfall nicht immer klar sein, was genau beachtet werden muss. Dies liegt zum Teil an der Tatsache, dass diese Art von Projekten üblicherweise nicht von Juristen durchgeführt wird.

Das vorliegende Dokument dient zur Unterstützung der Zuschussempfänger und möchte ihnen auf einfache Art darlegen wie sie vorgehen können um im Sinne des Datenschutzes zu arbeiten. Das Dokument ist jedoch rechtlich nicht bindend und dient lediglich der Orientierung.

Als oberste goldene Regel sollte immer das Gebot der Datensparsamkeit gelten. Ein Datum [1 Datum (Singular) / Daten (Plural)] welches ich nicht erhebe (und somit verarbeite), muss ich auch nicht schützen.

Die Datenverarbeitung beginnt bereits mit deren Speicherung. Wenn ich beispielsweise die Lieblingsfarbe meiner Teilnehmer:innen abfrage in einem Anmeldeformular und sonst nichts damit mache, dann habe ich trotzdem bereits eine Datenverarbeitung, im Sinne der DSGVO, durchgeführt.

Personenbezogene Daten

Aber welche Daten müssen eigentlich geschützt werden? Im Prinzip sind das alle Daten die es einer dritten Person erlauben, eine vorher unbekannte natürliche Person zu identifizieren bzw. näher zu bestimmen. Man spricht in diesem Fall von den „personenbezogenen Daten“. Daraus ergibt sich aber auch, dass Daten von Unternehmen wie bspw. die Adresse nicht dazu zählen.

Bei Angaben wie Wohnort und Alter leuchtet das ein aber manchmal ist es nicht ganz so offensichtlich. Beispielsweise kann auch die verwendete IP-Adresse im Internet zu den schützenswerten Daten gezählt werden. Diese Adresse wird benötigt damit jemand meine Webseite abrufen kann. In der Regel wird meine Webseite bzw. ein darauf installiertes Programm die Adresse des Besuchers speichern und ggf. im Nachhinein auswerten.

Aus diesen Vorgaben resultiert jedoch auch, dass Daten die nicht personenbezogen sind, nicht im Sinne der DSGVO geschützt werden müssen. Ich dürfte beispielsweise auf meiner Webseite eine Liste mit Unternehmen veröffentlichen die im Rahmen eines Sponsorings mein Projekt bezuschusst haben. Dazu benötige ich keine Einwilligung und ich muss auch nicht darüber informieren (siehe Punkt “Pflichten”). Jedoch dürfte ich nicht einfach einen Ansprechpartner “Herr Müller” namentlich nennen in dieser Liste.

Zeitlicher Rahmen

Oft stellt sich die Frage ab wann denn die DSGVO überhaupt greift. Sie wirkt sich aus ab dem Moment wo ich die Absicht habe Daten von Dritten zu erfassen (also zu speichern – elektronisch oder physisch spielt dabei keine Rolle).

Bei neuen Prozessen empfiehlt es sich also immer den DPO in der Planung einzubeziehen. Steht dieser aus welchen Gründen auch immer nicht zur Verfügung, dann gilt es die Punkte aus diesem Leitfaden zu beachten.

Der Datenschutz endet mit der gründlichen Vernichtung der personenbezogenen Daten. Es reicht nicht, beispielsweise eine Liste die sich auf Papier befindet zum Altpapier zu geben. Diese muss vorher durch ein geeignetes Gerät unwiderruflich zerstört werden (Aktenvernichter zum Beispiel). Ähnlich verhält es sich mit elektronischen Daten. Diese sind unwiderruflich zu löschen. Ein einfaches Verschieben in den Papierkorb (wie es unter Windows üblich ist) reicht nicht aus.

Für diese Aufgabe gibt es unter Windows eine breite Auswahl an Programmen. Die üblichen Suchmaschinen liefern bei den Begriffen “windows file shredder” eine große Liste an Treffern. Für andere Betriebssysteme gibt es natürlich ebenfalls Software die diese Aufgabe zuverlässig durchführt.

Pflichten

Informationspflicht vor Erhebung der Daten

Es gibt ein paar Punkte über die ich immer zum Zeitpunkt der Datenerhebung informieren muss:

- Den Namen und die Kontaktangaben des Verantwortlichen für diese Datenverarbeitung
- Ansprechpartner für den Datenschutz in meiner Organisation (Datenschutzbeauftragter; oft wird auch die englische Abkürzung DPO – data protection officer – verwendet)
- Was geschieht mit den Daten? Zu welchem Zweck werden die Daten erhoben?
- Auf welcher Rechtsgrundlage werden die Daten erhoben? Mehr dazu im Abschnitt “Rechtsgrundlage”
- Wie lange bleiben die Daten gespeichert?
- Wer erhält Zugriff auf diese Daten und mit welchem Ziel? An der Stelle sind außenstehende Firmen und Projetpartner gemeint. Es geht nicht darum mitzuteilen, dass Kollegin XY die Daten verwalten wird.

Egal wie ich später meinen Datenschutz entwerfe, es muss immer sichergestellt werden, dass ich die betroffenen Personen im Voraus darüber informiere. Dies ist unabhängig davon ob ich um Einwilligung in etwas bitte oder ob ich eine Angabe zur Erfüllung des Vertrags zwischen mir und den Teilnehmer:innen benötige.

Beispiel: Ich frage verschiedene persönliche Daten, bei der Anmeldung, ab um eine Liste mit Kontaktadressen zusammenzustellen. Die nutze ich um meinen Teilnehmern Nachrichten zukommen zu lassen (ich benötige dies um meinen Vertrag mit den Teilnehmer:innen zu erfüllen). Das wäre ein Punkt, der der Information dient, für die Datenschutz-Erklärung. Wenn ich während der Anmeldung auch noch abfrage ob die Teilnehmer:innen irgendwelche besonderen Bedürfnisse beim Essen haben (vegan, laktosefrei, …) dann muss ich sie darüber informieren, dass diese Informationen an ein Restaurant weitergeleitet werden in dem wir abends speisen werden.

In dem Beispiel dürfte ich im Nachhinein nicht hingehen und die Informationen bezüglich der Esspräferenzen anderweitig nutzen.

Ein anderes Beispiel: Auf einer Webseite arbeite ich mit einer Firma zur Auswertung der Nutzungsstatistiken zusammen. Dies muss in meiner Datenschutzerklärung auf der Webseite vermerkt sein.

Die Informationen müssen den betroffenen Personen mitgeteilt werden – idealerweise schriftlich. Am besten lässt man sich den Erhält der Erklärung auch noch quittieren. Folgenden Satz könnte man unten auf ein entsprechendes Formular drucken und der Person in Kopie aushändigen:

> Ich wurde über die Verarbeitung meiner Daten belehrt und nehme meine daraus entstandenen Rechte (Korrigierbarkeit, Einsicht) zur Kenntnis. Ich habe eine Kopie der oben genannten Belehrungen erhalten.

Informationspflicht bei IT-Zwischenfällen

Sollte es zu einem Zwischenfall in meiner Einrichtung kommen, dann muss ich unverzüglich – in spätestens 72 Stunden – alle Betroffenen informieren, dass ihre Daten bspw. unberechtigt kopiert wurden. Ich muss ebenfalls die Datenschutzaufsichtsbehörde informieren. Dies wird über ein Formular erledigt welches ich auf der Webseite herunterladen kann. Ironischerweise benötigt man ausdrücklich den Adobe Reader dazu: https://www.autoriteprotectiondonnees.be/professionnel

Die folgende Liste enthält Beispiele für “IT-Zwischenfälle”

- Unbefugte haben sich Zugriff auf meine IT-Infrastruktur verschafft und wären in der Lage gewesen Daten zu kopieren (oder haben sie sogar nachweislich kopiert).
- Ein Laptop wurde gestohlen oder es wurde irgendwo vergessen (im Zug bspw.) und auf diesem befanden sich sensible Daten. Der Datenträger war nicht verschlüsselt.
- Sie stellen fest, dass eine Ihrer Listen mit Namen im Internet frei aufrufbar ist.
- Bei einem von Ihnen, mit der Verarbeitung beauftragten Unternehmen kommt es zu einem Zwischenfall.
- Sie löschen versehentlich die Daten Ihrer Teilnehmer:innen und besitzen kein Backup (nicht mal mit älteren Versionen der Daten)

Die Rechte der Organisation

Ich darf alle Daten erheben die ich zur Erfüllung eines Vertrags zwischen einer natürlichen Person und meiner Organisation benötige. Beispielsweise beim Buchen eines Flugs, ist es mittlerweile unerlässlich, den Namen, Vornamen und Nummer des Ausweises der Fluggesellschaft im Vorfeld mitzuteilen. Das entbindet mich jedoch nicht von meiner Informationspflicht.

Zusätzlich kann ich mich unter bestimmten Bedingungen auf ein berechtigtes Interesse berufen personenbezogene Daten zu erheben. Wenn ich eine Weiterbildung veranstalte, dann habe ich ein berechtigtes Interesse ein Gruppenfoto zu PR-Zwecken zu erstellen.

Rechtsgrundlage

- die betroffene Person kann ihre Einwilligung dazu erteilen;
- die Verarbeitung ist aufgrund eines Vertrags erforderlich – dieser muss nicht unbedingt mit einer Bezahlung einher gehen;
- die Verarbeitung erfolgt aufgrund einer gesetzlichen Verpflichtung;
- die Verarbeitung ist erforderlich um lebensnotwendige oder gesundheitliche Vorkehrungen treffen zu können - üblicherweise sind davon Ärzte und Krankenhäuser betroffen
- die Polizei im Rahmen ihrer Tätigkeit

Verhalten

Es ist immer schwierig den Überblick über alle Regeln zu behalten und diese zu beachten. Darum folgen hier ein paar praktische Tipps um sich “korrekt zu verhalten”:

- E-Mail, wie es heute üblicherweise verwendet wird, ist kein vertrauenswürdiger Weg zur Übermittlung von personenbezogenen Daten. Eine einfache Alternative wäre, die Daten mit einem Programm wie “7-Zip” zu einem verschlüsselten Archiv zusammen zu fassen und dann zu verschicken.
- Die übliche Verwendung von Datenträgern stellt ein ähnliches Datenschutzproblem dar: viele Menschen verschlüsseln ihre Daten zum Austausch und Backup nicht. Es gibt jedoch für alle Betriebssysteme mehrere Programme die diese Aufgabe übernehmen können. Die Suchmaschine Ihres Vertrauens wird ihnen eine riesige Auswahl liefern. Im Jugendbüro verwenden wir “Veracrypt” (https://www.veracrypt.fr/en/Home.html) und haben damit gute Erfahrungen gemacht.
- Speichern Sie die Daten an einem zentralen Ort und sichern Sie diesen regelmäßig! Backups sind nicht nur wegen der DSGVO eine gute Idee. Die Cloud ist kein Backup!
- Passwörter ergeben nur einen Sinn, wenn sie gut sind. Ein gutes Passwort hat mindestens 10 Zeichen und enthält Groß-, Kleinbuchstaben, Ziffern und Sonderzeichen.
- Passwörter die im Browser gespeichert werden sind nicht sicher! Hier müssen Sie abwägen wie wichtig die Daten sind auf die Sie zugreifen.
- Wenn Sie den PC verlassen, dann sperren Sie bitte den Bildschirm!
- Wenn Sie mit anderen Organisationen zusammenarbeiten, dann stellen Sie schriftliche Vereinbarungen auf. Wir haben eine minimale Vorlage die Sie um weitere, eigene Punkte erweitern können.

Glossar

DPO Abkürzung für Data protection officer – damit ist der Datenschutzbeauftragte gemeint. Auch im Deutschen verwendet man häufig diese Abkürzung da es keine adäquate Entsprechung gibt.

DSGVO Abkürzung für Datenschutz Grundverordnung