Stadt Bern

ombuds stelle daten schutz

Effingerstrasse 4
3011 Bern
Telefon 031 312 09 09

ombudsstelle@bern.ch
datenschutz@bern.ch

Datenschutzkonforme Projektkonzipierung – ein Kurzüberblick

Dieses Dokument soll Ihnen einen Kurzüberblick darüber verschaffen, welche datenschutzrechtlichen Grundsätze Sie schon ganz zu Beginn eines IT-Projekts berücksichtigen sollten, damit die Produktentwicklung und der Betrieb der Applikation möglichst datenschutzfreundlich verlaufen kann. Alle im IT-Projekt involvierten Personen sollen mittels dieses Kurzüberblicks dahingehend sensibilisiert werden, um mögliche Datenschutzrisiken rechtzeitig zu erkennen und gegebenenfalls entsprechende Massnahmen ergreifen zu können. Denn bereits während des IT-Projekts gilt es im Sine von «privacy by design» Datenschutz-Risiken frühzeitig zu erkennen und zu beheben, damit das städtische IT-Produkt auch tatsächlich und ressourcenschonend zum Einsatz kommen kann.
Bitte nehmen Sie zur Kenntnis, dass dieses Dokument keine Vollständigkeit beansprucht und jedes IT-Projekt individuell auf seine Datenschutzkonformität überprüft werden muss. Weiterführende Informationen finden Sie **hier** oder im direkten Kontakt mit der Datenschutz-Aufsichtsstelle.

Datenbearbeitung nur mit rechtlicher Grundlage

Städtische Behörden dürfen Personendaten nicht ohne Legitimation bearbeiten. Wenn Sie in ein IT-Projekt einsteigen, vergewissern Sie sich, dass die geplante Datenbearbeitung eine rechtliche Grundlage hat. Der Erlass, auf den Sie Ihre Datenbearbeitung stützen, muss die Datenbearbeitung also ausdrücklich erlauben oder das Bearbeiten muss der Erfüllung einer im Gesetz genannten Aufgabe dienen (Art. 5 Abs. 1 KDSG, BSG 152.04). Wenn Sie sehr sensible Daten über Personen bearbeiten, sogenannte besonders schützenswerte Personendaten, dann muss sich aus dem Gesetz *klar ergeben*, dass die Daten bearbeitet werden dürfen, oder das Bearbeiten muss zur Erfüllung einer gesetzlichen Aufgabe *zwingend erforderlich sein* (Art. 6 Abs. 1 lit. a und b KDSG).

Datenbearbeitung nur nach vordefiniertem Zweck

Bevor Sie Ihr IT-Produkt implementieren und dazu die notwendigen Personendaten erheben, müssen Sie sich bewusst machen, zu welchem Zweck das Produkt überhaupt eingesetzt werden soll. Die von Ihnen erhobenen Daten dürfen dann – mit wenigen Ausnahmen – nur noch zu diesem Zweck bearbeitet werden (Art. 5 Abs. 2 und 4 KDSG). Eine Zweckentfremdung stellt also ebenfalls eine Datenschutzverletzung dar.

Sie wollen die Fahrzeuge des Winterdienstes mit einem GPS-Trackingsystem ausstatten, um ermitteln zu können, welche Strassen noch vom Schnee befreit werden müssen. Die Standort-Daten werden also zum Zweck der Strassenwartung im Winterdienst erhoben. Dies bedeutet, dass diese Daten zu keinem anderen Zweck bearbeitet werden dürfen. Nicht gestattet ist demnach, dass Sie mit diesen Daten zusätzlich Ihre Angestellten kontrollieren. Sie sind also auch angehalten Ihr IT-Produkt mit jenen technischen und organisatorischen Massnahmen auszugestalten, damit eine Zweckentfremdung verunmöglicht wird.

Verhältnismässige Datenbearbeitung

Wenn städtische Behörden Personendaten bearbeiten wollen, muss die Bearbeitung verhältnismässig sein (Art. 5 Abs. 3 KDSG). Ob eine Datenbearbeitung verhältnismässig ist, kann jeweils nur im Einzelfall beurteilt werden.

Wichtig ist, dass Ihr angestrebtes IT-Produkt überhaupt geeignet ist, den Zweck zu erfüllen, der damit verfolgt wird.

Sie verfolgen ein Projekt, das eine automatisierte Ermittlung von Adressdaten ermöglichen soll, damit den Finder*innen von Fundgegenständen die Adressdaten der Besitzer*innen ohne Kontakt zum Fundbüro zugestellt werden können. Wenn Ihr IT-Produkt die Daten nicht korrekt verknüpfen kann, eignet es sich bis zur Behebung der Fehlfunktion nicht zur automatisierten Vermittlung der Adressdaten und darf bisweilen nicht zum Einsatz kommen.

Ihr angestrebtes IT-Produkt muss zudem erforderlich sein, um den Zweck zu erfüllen, den es verfolgt. An dieser Stelle gilt es immer zu fragen, ob andere Lösungen die Privatsphäre und den Persönlichkeitsschutz der Bürger*innen weniger tangieren. Ebenso ist zu prüfen, ob ein IT-Produkt tatsächlich mehr Effizienz bietet oder ob allenfalls auch andere, weniger grundrechtseingreifende Lösungen zum gewünschten Ziel führen. Auch stellt sich regelmässig die Frage, ob überhaupt Personendaten von so vielen Bürger*innen gesammelt werden sollen und dürfen. Denn ein wichtiger Aspekt der Erforderlichkeit ist, dass nur die Menge an Personendaten gesammelt werden darf, die tatsächlich notwendig ist.

Sie wollen die Adressdaten aller städtischen Bürger*innen in Ihr Produkt zur Adress-Ermittlung migrieren, um sicher zu stellen, dass nur korrekte Adress-Informationen in die Web-Maske eingesetzt werden können. Dieses Vorgehen wäre jedoch unverhältnismässig und deswegen unzulässig, weil es auch datensparsamere Möglichkeiten gäbe, um den Zweck der automatisierten Kontakt-Vermittlung zu ermöglichen. Datenschutzfreundlicher ist es, wenn sowohl die Finder*innen der Fundgegenstände als auch die Besitzer*innen eigenhändig und freiwillig ihre Adress-Daten übermitteln.

Sodann müssen Sie sicherstellen, dass Ihr Produkt den Bürger*innen überhaupt zugemutet werden kann. Dies ist nur dann der Fall, wenn der verfolgte Zweck, also bspw. eine effiziente Fundvermittlung, die möglichst ressourcenschonend sein soll, deutlich wichtiger erscheint als der Privatsphären- und Persönlichkeitsschutz der Bürger*innen.

Ihr Produkt zur Adress-Ermittlung soll das städtische Fundbüro weitestmöglich ablösen. Deswegen sollen alle Adress-Daten der städtischen Bürger*innen in das Produkt migriert werden. Finder*innen, die Gegenstände mit einem Personenbezug, bspw. ein Portemonnaie, auffinden, können über Ihr IT-Produkt eine Personennachforschung betreiben. So können etwa über die Eingabe des auf der Identifikationskarte geführten Namens die Kontakt- oder gar Adressinformationen der Besitzer*innen ermittelt werden. Dieses Vorgehen wäre im Lichte der Privatsphären- und des Persönlichkeitsschutzes unzumutbar, da Kontakt- oder Adressdaten nicht ohne die Einwilligung der Besitzer*innen weitergegeben werden dürfen.

Datensicherheit

Die durch das IT-Produkt bearbeiteten Personendaten müssen durch angemessene technische und organisatorische Massnahmen gegen unbefugtes Bearbeiten geschützt werden.
Die Massnahmen müssen aber auch dahingehend Schutz bieten, dass das Produkt fehlerfrei funktioniert und es etwa zu keinem Datenverlust kommt. Die Datensicherheit ist gegeben, wenn die Vertraulichkeit, die Verfügbarkeit sowie die Datenintegrität bzw. Datenrichtigkeit über den ganzen Lebenszyklus der Daten sichergestellt sind.

Vertraulichkeit: Anhand technischer Massnahmen und organisatorischen Vorkehrungen, stellen Sie sicher, dass nur diejenigen Personen Zugriff auf die vorhandenen Daten haben, die auch dazu berechtigt sind und diese zur Erfüllung ihrer gesetzlichen Aufgaben zwingend benötigen. Beispielmassnahmen: Zugangskontrolle, Zugriffskonzept, Verschlüsselung, Mehrfachauthentifizierung.

Verfügbarkeit: Die Personendaten müssen in der gewünschten Form und zum gewünschten Zeitpunkt für die Zugriffsberechtigten verfügbar sein, ansonsten ist Ihr Produkt für die Zweckerfüllung nicht hinreichend geeignet, wodurch auch der Grundsatz der Verhältnismässigkeit verletzt wäre. Beispielmassnahmen: Redundante Auslegung der Systemlandschaft, geeignete Datensicherung, Definition vertretbarer Ausfallszeiten.

Datenintegrität bzw. Datenrichtigkeit: Ihr angestrebtes IT-Produkt darf nur korrekte Daten bearbeiten. Daraus folgt, dass die datenbearbeitende Behörde auch die Pflicht trägt, sicherzustellen, dass nur richtige und vollständige Daten in das IT-Programm migriert und dass Daten nicht unbefugt verändert werden können resp. zumindest erkannt wird, dass Veränderungen vorgenommen wurden. Zudem stehen Sie in der Pflicht, technische und organisatorische Massnahmen einzuführen, die es gestatten, die Daten aktuell zu halten. Stehen etwa Schnittstellen im Einsatz, die verschiedene IT-Produkte zusammenschliessen, muss sichergestellt sein, dass Änderungen am Grunddatenbestand auch in den Anschlussprodukten übernommen werden. Beispielmassnahmen: Rollenbasiertes Berechtigungskonzept, angemessenes Logging, Verschlüsselung der Daten.

Datenbearbeitung durch Dritte

Städtische Behörden können nicht alle IT-Programme selbständig entwickeln und warten, weshalb sie immer auf die Unterstützung Dritter, vornehmlich privater Unternehmen, angewiesen sind. Teilweise werden IT-Dienstleistungen auch vollständig aus dem städtischen Umfeld ausgelagert und von privaten Unternehmen übernommen. Die datenbearbeitende Behörde bleibt jedoch auch bei einer sogenannten Auftragsdatenbearbeitung durch Dritte vollumfänglich für den Datenschutz verantwortlich (Art. 8 Abs. 1 KDSG). Demnach bleiben Sie allen hier umschriebenen Datenbearbeitungsgrundsätzen weiterhin verpflichtet bzw. Sie müssen sicherstellen, dass anhand eines Auftragsdatenbearbeitungsvertrag und einer entsprechenden Datenschutzbestimmung der Schutz der Daten bei der Bearbeitung durch Dritte auch tatsächlich gewährleistet ist. Eine Abtretung der Verantwortung ist deshalb nicht möglich.

Auch Cloud-Dienstleistungen gelten als Auftragsdatenbearbeitung durch Dritte. Diese Form der Auftragsdatenbearbeitung untersteht jedoch einem erhöhten Risiko, da die Cloud-Server teilweise im Ausland liegen und dadurch bspw. das Datenschutzrecht ausländischer Staaten Anwendung findet. Ausführliche Informationen zu cloud-spezifischen Risiken und Massnahmen finden Sie **hier**.

Grundsätzlich, und unabhängig vom Einsatz von Cloud-Dienstleistungen mit Auslandsbezug, müssen Sie all jenen IT-Projekten Beachtung schenken, die eine grenzüberschreitende Datenbearbeitung vorsehen. Eine relevante Voraussetzung, um personenbezogene Daten an Empfangende im Ausland weitergeben zu dürfen, ist, dass im Empfängerland eine Gesetzgebung existiert, die ein angemessenes Datenschutzniveau durchsetzt (**zur Staatenliste**).