

INHALTSVERZEICHNIS

Datenschutz-Grundverordnung	2
Schutzmassnahmen	2
Auskunftsrecht	3
Änderungswünsche	4
Löschanfragen	5

DATENSCHUTZ-GRUNDVERORDNUNG

Ab Ende Mai 2018 tritt die EU Datenschutz-Grundverordnung (DS-GVO, englisch GDPR) in Kraft. Sie gilt und hat Folgen für alle, die personenbezogene Daten von EU Bürgern verarbeiten, gleich ob dies innerhalb oder außerhalb der EU passiert. Wir und Sie sind also in der Pflicht, uns an die Vorschriften der DS-GVO zu halten und genießen privat auch den Schutz aus dieser Verordnung.

Hier finden Sie den Wortlaut der Verordnung: <https://dejure.org/gesetze/DSGVO>

Gleichzeitig sind Gewerbetreibende und die Anwender unserer Software im Zweifel auch immer direkt betroffen, denn wir verarbeiten in unserer Software personenbezogene Daten. Dazu zählen nämlich auch schon Email-Adressen und damit selbst fast anonyme Kundenanfragen via Kontaktformular. Bei der Speicherung und Nutzung von Name, Vorname, Straße, PLZ und Ort gibt es dann überhaupt kein Vertun. Und auch alle „angehängten“ Daten wie Aufträge, Angebote, Notizen oder Abrechnungen zählen zu den personenbezogenen Daten.

Um DS-GVO konform zu arbeiten, sind eine Reihe von Bedingungen zu erfüllen. Einige davon sind organisatorischer Art, andere betreffen die Veröffentlichung von Datenschutz-Richtlinien und den Kontaktdaten von Datenschutz-Verantwortlichen sowie die Einholung von Einwilligungen zur Datenverarbeitung von Ihren Kunden, Interessenten, Mietern etc.

Eine Checkliste finden Sie z.B. hier: <https://www.haendlerbund.de/de/leistungen/rechtssicherheit/agb-service/datenschutzgrundverordnung/checkliste>

Und einen Einstieg hier: https://www.gdd.de/downloads/praxishilfen/GDD-Praxishilfe_DS-GVO_8.pdf

An den beiden Stellen dürften Sie schnell erkennen, dass die Aufgabenstellung, sich an die Vorschriften der DS-GVO kein leichtes Unterfangen und nicht mal eben schnell und zwischendurch zu erledigen ist.

Kommen wir nun zu der Frage, was unsere Software zur Einhaltung der DS-GVO beiträgt bzw. wie Sie unsere Software DS-GVO konform einsetzen können.

SCHUTZMASSNAHMEN

Zuallererst sollten Sie natürlich ausschließen, dass Unbefugte Zugriff auf die von Ihnen gespeicherten und verarbeiteten Daten haben. Dabei unterstützt Sie unsere Software mit folgenden Merkmalen:

- Ausschließlich verschlüsselte Datenübertragung zwischen Server und Client (SSL/https Verschlüsselung im Standard bei unseren Hosting-Angeboten)
- Zugang zur Anwendung ausschließlich mit Benutzername und Passwort, wobei ein „sicheres“ Passwort bei der Registrierung software-technisch verlangt wird.
- Wir als Ihr Beauftragter in der Auftragsdatenverarbeitung stellen Ihnen eine [Vereinbarung zur Auftragsdatenverarbeitung](#) gemäß Muster des Bundesministeriums des Inneren zur Verfügung. Damit können Sie a) sichergehen, dass wir uns ebenfalls an die DS-GVO halten und Sie können dies b) auch jederzeit damit belegen. Wir unsererseits haben eine entsprechende Vereinbarung mit unserem Rechenzentrum ([All-Inkl. in Deutschland](#)). Somit können Sie von rechtskonformen Prozessen bei uns ausgehen und sind rechtlich auf der sicheren Seite.
- Unsere Software verfügt über ausgefeilte Mechanismen zum Datenschutz und hier vor allem zur Verwaltung von Zugriffsrechten für Ihre Mitarbeiter. Diese zu nutzen und sinnvoll im Sinne der DS-GVO umzusetzen obliegt Ihnen – wir können nur die Werkzeuge liefern. In jedem Fall aber können Sie Mitarbeitern den Zugriff ganz untersagen, den Zugriff nur auf bestimmte Module und Auswertungen gewähren, die Möglichkeit zur Veränderung der Datenbestände nehmen und Datensätze vom Zugriff ausschließen: [Benutzerrechte-Verwaltung ...](#)

- Weiterhin können Sie davon ausgehen, dass unsere Software von sich aus keine gesetzeswidrigen Aktivitäten entfaltet. Es werden also „unter der Haube“ keine Analysen und Auswertungen gefahren, die Ihnen nicht zur Kenntnis gelangen. Schon gar nicht findet eine Datenweitergabe an Dritte statt. Lediglich zu Zwecken der Software-Entwicklung und -pflege und im Support kann es notwendig werden, dass administrativ – aber immer unter Berücksichtigung der DS-GVO - ausschließlich von dazu berechtigten Mitarbeitern der INTex Publishing GmbH & Co. KG (siehe Auftragsdatenverarbeitung im Falle des Hostings durch uns) zugegriffen wird. Sie können also davon ausgehen, dass Datenverarbeitung nur zu den Zwecken stattfindet, zu denen unsere Software programmiert wurde und zu denen sie angeboten wird. Irgendwelche Backdoors gibt es nicht. Unser Geschäftsmodell bezieht sich auf den Verkauf von Software an Sie, nicht auf den Verkauf von Daten jedweder Art.
- Datensparsamkeit ist ein Anliegen der DS-GVO – es soll nur gespeichert werden, was auch gespeichert werden muss. Dies teilen wir, können aber software-technisch hierzu wenig beitragen. In jedem Fall ist die Datenbankstruktur so ausgelegt, dass nach Möglichkeit an keiner Stelle eine doppelte Datenhaltung erfolgt oder gar versteckt Daten gespeichert werden. Was Sie und Ihre Mitarbeiter aber etwa in Bemerkungen-Feldern speichern, liegt nicht in unserer Hand und sollte administrativ durch Sie geprüft werden. Sie sollten hier Ihre Mitarbeiter auch zur Zurückhaltung auffordern. Wegen des Auskunftsrechts kann sonst eine Bemerkung wie „Dummkopf“ oder „Frechdachs“ in der Datenbank schnell zum Problem werden.
- Eine solche Prüfung wird dadurch erleichtert, dass vielfach für wichtige Daten der Datenerfasser und der Datenbearbeiter mit Datum der letzten Bearbeitung sichtbar im Frontend gespeichert wird. Zusätzlich wird im Backend ein Audit geschrieben, aus dem sich alle Logins und Veränderungen an Datensätzen nachvollziehen lassen. Aktivitäten lassen sich bei Bedarf also einem Nutzer zuordnen. Natürlich nur solange, wie Sie auch für jeden physischen Nutzer einen getrennten Nutzer-Account mit eigenem Login gebucht bzw. angelegt haben und Benutzer-Zugänge nur jedem einzelnen Mitarbeiter bekannt sind. Das ist aber wieder eine organisatorische Frage, die wir mit Software nicht lösen können.
- Wenn Sie Daten aus unterschiedlichen Quellen beziehen – etwa Shop, Kontaktformular, Telefon und Fax -, dann können und sollten Sie die Herkunft dieser Daten und evtl. damit verbundene Einwilligungen dokumentieren. Speichern Sie etwa schriftliche Anfragen als Dokument als Anhang zur Adresse im Organizer-Teil des Programms. Oder nutzen Sie eines der frei definierbaren Detailfelder im Adressmodul für diesen Zweck. INTex Adressen PLUS, INTex Hausverwaltung PLUS und INTex Auftrag PLUS verfügen zu diesem Zweck über ein gesondertes Feld „Datenherkunft“ und speichern das Datum der Ersterfassung automatisch.
- Für die Speicherung besonders sensibler Daten gibt es in INTex Adressen PLUS, INTex Hausverwaltung PLUS und INTex Auftrag PLUS fünf „vertrauliche“ Felder, deren Inhalt in der Datenbank verschlüsselt gespeichert werden und die auch nur in der Ansicht „Adressen (vertraulich)“ überhaupt sichtbar sind. Diese Ansicht kann „normalen“ Mitarbeitern über die Zugriffsrechte vorenthalten werden. Die Daten sind auch nicht exportierbar und im Backend der Datenbank nur verschlüsselt zu sehen. Eine Nutzung via ODBC oder API-Zugriff ist wegen der Verschlüsselung ausgeschlossen. Das Modul wird in einem neuen Fenster/Tab geöffnet, um ein einfaches Zurück-Navigieren für Unbefugte zu verhindern.

AUSKUNFTSRECHT

Gemäß Art. 15 der DS-GVO hat Ihr Kunde/Interessent/Mieter ein Auskunftsrecht darüber, was über ihn in Ihrer EDV gespeichert wurde und wie diese Daten genutzt werden. Sie müssen also jederzeit dazu in der Lage sein, dem Berechtigten eine entsprechende Auskunft über die bei Ihnen von ihm gespeicherten Daten erteilen. Diese Auskunft kann recht umfangreich werden, wenn Sie auch an alle verknüpften Daten wie Aufträge, Angebote, Lieferscheine, Dokumente, Notizen, Verträge etc. denken. Zudem muss die Auskunft auch in maschinenlesbarer Form – also digital erfolgen.

Folgende Hilfen bietet die INTex Software:

- Zunächst hilft es schon sehr, wenn Sie unsere Software als zentrale Daten-Plattform verwenden, d.h. alle Daten nur hier und nirgendwo anders speichern. Das erspart Ihnen das Suchen und Zusammentragen unterschiedlicher Daten aus diversen Quellen.
- In der Adressverwaltung können Sie den Anfragersteller über Name, Anschrift, Email, Kundennummer und andere Angaben schnell und zuverlässig finden, identifizieren und sicherstellen, dass es sich um niemand anderes als den Anfragersteller handelt. Sie sollten unbedingt gewährleisten, dass sich der Anfragersteller eindeutig identifiziert bzw. Ihnen von Person bekannt ist.
- Im Ansichtsbildschirm der Adresse sind gleich auch immer alle verknüpften Daten sichtbar. Sie können also feststellen, ob zusätzlich zu den eigentlichen Adressdaten auch weitere Daten wie Notizen, Aufträge, Abrechnungen etc. gespeichert wurden.
- Alle Datensätze sind über eine Abfrage in den jeweiligen Modulen jederzeit auszufiltern und können dann gedruckt oder im Excel- oder Text-Format (ASCII CSV) gespeichert werden. Diese Exportdateien können Sie dem Anfragersteller zur Verfügung stellen. Hierbei sollte auf einen Versand per Mail verzichtet werden, weil dies alle Sicherheitsbemühungen ad absurdum führen würde. Auch eine Speicherung auf außer-europäischen Cloud-Diensten und Verlinkung zu diesen ist alles andere als ratsam. Ein Download-Angebot von Ihrer eigenen Website (SSL-verschlüsselt) oder der postalische Versand eines Datenträgers mit den Daten sollte die Bedingungen erfüllen.

Bei den Server-Versionen kann sich der Administrator den Export der verschiedenen Daten über MySQL Dump oder ein SQL Script etwa in Workbench wesentlich erleichtern. Der –where Parameter von Dump erlaubt den Export nur von bestimmten Daten, also etwa allen Daten mit Bezug auf Adresse A in allen Tabellen. Mit einem Script und der Select Option into outfile können Sie ebenfalls bestimmte Daten automatisiert in Dateien schreiben.

Für die Rückantwort sollten Sie ein standardisiertes Schreiben verwenden, um nichts zu vergessen.

Muster eines Auskunftsschreibens gemäß DS-GVO: <https://www.formblitz.de/products/selbstauskunft-zur-verarbeitung-personenbezogener-daten-dsgvo.html>

Oder kostenlos hier: https://synaxon.ag/uploads/media/DSGVO_Artikel15_Auskunftsrecht.pdf

ÄNDERUNGSWÜNSCHE

Der „Dateninhaber“ kann eine Änderung der bei Ihnen gespeicherten Daten verlangen. Bei einer einfachen Änderung etwa der Anschrift kann dies keinerlei Problem und auch in Ihrem Sinne sein, denn wenn die Adresse etwa wegen Umzug nicht mehr stimmt, sind Sie über eine Korrektur sogar froh, damit das nächste postalische Mailing nicht im Nirwana landet.

Selbstverständlich können Sie zu solchen Zwecken in der INTex Software die entsprechenden Daten jederzeit ändern. Den Auftrag zur Änderung sollten Sie sicherheitshalber dokumentieren (Organizer/Dokumente).

Es gibt aber möglicherweise eine Reihe von gespeicherten Daten, die Sie aus inhaltlichen oder rechtlichen Gründen nicht ändern können oder gar dürfen. Nur einige Beispiele:

- Wegen der Vorschriften ordnungsgemäßer Buchführung können Sie selbst fehlerhafte Buchungen nicht einfach ändern, sondern müssen diese stornieren – die fehlerhafte Buchung bleibt nachvollziehbar erhalten, wird aber durch den Storno wertmäßig aufgehoben. Das kann und darf auch auf Kundenwunsch hin nicht geändert werden.
- Rechnungen sind nach den Vorgaben des Finanzamtes nicht zu manipulieren, um Ihrer Umsatzsteuerpflicht zu genügen. Daher dürfen Sie eine Rechnung – einmal gedruckt und versandt – auch nicht mehr einfach ändern und noch mal verschicken. Nur der Storno der Erstrechnung und die Erstellung einer zweiten, neuen Rechnung erfüllt die Bedingungen der Finanzbehörden.

In derartigen Fällen ist es bei unserer Software teilweise auch gar nicht möglich, Datensätze noch nachträglich zu verändern – verbuchte Buchungen lassen sich nur noch stornieren.

LÖSCHANFRAGEN

Neben dem Auskunfts- und Korrektur-Recht hat der Dateninhaber ein Recht auf „Vergessen-werden“, d.h. er hat unter Umständen einen Anspruch darauf, komplett aus Ihren Daten zu verschwinden – dauerhaft und auch in allen Kopien und Backups.

In der Praxis werden dem aber - zumindest bei allen Kunden und Mietern - andere Vorschriften entgegenstehen. Für alle steuerrelevanten Daten beispielsweise gilt eine 10jährige Archivierungspflicht Ihrerseits.

Mehr zu den Archivierungspflichten hier: https://www.hk24.de/produktmarken/beratung-service/recht_und_steuern/steuerrecht/abgabenrecht/aufbewahrungsfristen-geschaeftsunterlagen/1157174

Wenn also jemand bei Ihnen etwas gekauft hat und dieser Kauf nicht mehr als 10 Jahre her ist, dann können Sie einem Löschwunsch dieser Daten nicht nachkommen. Lediglich bei Daten, die über den reinen Kaufhergang hinausgehen wie z.B. im Kundengespräch herausgefundene Präferenzen des Kunden für Produkte einer bestimmten Art und Güte könnten entfernt werden.

Da, wo es aus rechtlichen Gründen möglich ist, können Sie in der INTex Software auch immer Daten löschen. Bei den Server-Versionen kann sich der Administrator das Löschen in mehreren Tabellen über ein SQL Script etwa in Workbench wesentlich erleichtern.

Wenn die Löschung rechtmäßig verlangt wurde, dann hat diese schon zu Ihrem eigenen Schutz unmittelbar und vollständig zu erfolgen – nicht, dass Sie den Betreffenden am folgenden Tag noch mit unerwünschter Werbung behelligen. Knackpunkt beim Löschen werden allerdings neben den eigentlichen Daten in der Datenbank alle exportierten Daten und die Backups sein.

Sie sollten Exporte daher nach Möglichkeit über Benutzerrechte auf einen möglichst kleinen Anwenderkreis einschränken. Eventuell ist bei Cloud-Hostings und Server-Installationen der [ODBC-Zugriff](#) eine Alternative, weil hier live auf die Daten zugegriffen wird und somit keine Datenkopie entsteht. Allerdings könnte der Anwender hier immer noch eine lokale Kopie erzeugen, selbst dann, wenn es keine Notwendigkeit dazu gibt.

Beim Backup kann es schwierig werden, wenn das Backup in Form einer nicht zu bearbeitenden Kopie der Datenbank stattfindet. Empfehlenswerter im Sinne der DS-GVO ist es wohl, das Backup in Form einer gespiegelten Datenbank darzustellen. Alle Löschungen in der Haupt-Datenbank spiegeln sich dann alsbald in der Kopie bzw. können analog zur Produktionsdatenbank auch in der Kopie durchgeführt werden. Damit dies aber nicht zu unerwünschten Datenverlusten führt, sollte über Benutzerrechte das Löschen von Daten nur wenigen Mitarbeitern überhaupt erlaubt werden und eventuell ist die Einhaltung des Vier-Augen-Prinzips hier ratsam.

Schließlich sollten Sie auch durch Daten-Synchs entstandene Kopien in der Cloud bedenken. Auf diese haben Sie oft keinen direkten Zugriff, was die Sache erschwert. Der Einsatz einer zentralen Datenbank – wie es bei den INTex Lösungen der Fall ist – ist im Sinne der Löschansprüche durch die DS-GVO in jedem Fall dezentraler Datenhaltung mit unzähligen Synch-Instanzen vorzuziehen. Der unkontrollierte Adressdaten-Synch über US-amerikanische oder andere außer-europäische Provider kann für die Einhaltung der DS-GVO zu einem ernsthaften Problem werden.