

gotomaxx
maximum



Schon wieder Gesetzesänderungen?!

DSGVO und ZUGFeRD verändern die Prozesse
in allen Unternehmen

Bereit für die Gesetzesänderungen 2018



Bald ist es so weit – ab dem 25. Mai 2018 gilt die neue Datenschutz-Verordnung (DSGVO) in allen EU-Mitgliedsstaaten und wird damit Teil der nationalen Rechtsordnung sein.

Als Unternehmen für Softwareentwicklung bedeutet das für uns gleich in zweierlei Hinsicht Umdenken, Anpassen und Neudenken. Denn zum einen ist gotomaxx ein Unternehmen, das EU-weit Produkte und Leistungen vertreibt und damit selbst allen Anforderungen der DSGVO entsprechen muss. Und zugleich stehen wir vor der Herausforderung, unsere Software & Services so anzupassen, dass es unseren Anwendern möglichst leicht gemacht wird, ihrerseits im Sinne der DSGVO zu agieren.

Deshalb befasst sich die aktuelle maximum auch primär mit Themen rund um die DSGVO, zum Beispiel mit DSGVO-konformen Funktionen wie der Verschlüsselung von PDF-Dateien im PDFMAILER 6.1. Auch das Thema Digitalisierung rückt wieder in den Fokus. Denn ab November 2018 wird für öffentliche Auftraggeber die elektronische Rechnung verpflichtend. Mit dem PDFMAILER 6.1 lässt sich die sogenannte XRechnung erstellen, die als deutsches Standardformat für elektronische Rechnungen anerkannt ist. Johannes Bisson von gotomaxx gibt Auskunft, inwieweit die DSGVO Einfluss nimmt auf die Unternehmen, aber auch dazu, welche Auswirkungen die neue Verordnung auf Produkte

und bestimmte Funktionen hat und welche gezielten Angebote es gibt, um Sie zu informieren.

Uns liegt viel daran, Sie bestmöglich zu unterstützen und Sie fit zu machen für die Neuerungen, die die DSGVO mit sich bringt. IT-Sicherheit war allerdings schon immer ein wichtiges Thema für uns und viele Aspekte, die die DSGVO fordert, sind bereits seit längerem Bestandteil unserer Produkte.

Nehmen Sie sich Zeit für diese Ausgabe der maximum – es ist wichtig vorbereitet zu sein auf den 25. Mai 2018.

Viel Spaß beim Lesen wünscht

Matthias Neumer
Geschäftsführer

Impressum

 **gotomaxx software GmbH**
Alte Bundesstraße 16 • 76846 Hauenstein

Telefon: +49 (0) 63 92 - 995 100

www.gotomaxx.com
maximum@gotomaxx.com

Geschäftsführer: Matthias Neumer, Dirk Winter
Redaktion: Corinna Müller, Daniel Frech
Layout: David Bohl

Urheberrechte: Die im Magazin enthaltenen Beiträge sind urheberrechtlich geschützt. Alle Rechte werden vorbehalten. Redaktionelle Beiträge geben nicht unbedingt die Meinung des Herausgebers wieder.

Hinweise und Warenzeichen (*): Andere, nicht gotomaxx eigene Produktnamen oder Firmenbezeichnungen sind Warenzeichen oder eingetragene Warenzeichen ihrer berechtigten Eigentümer.



Die DSGVO auf den Punkt gebracht

Die neue Datenschutz-Grundverordnung der EU (EU-DSGVO) gilt ab dem 25.05.2018. Die DSGVO reformiert und vereinheitlicht die Prozesse, die mit der Erhebung und Verarbeitung personenbezogener Daten zusammenhängen. Diese Verordnung konkretisiert bestehende Verordnungen und gleicht die nationalen Gesetze einander an. In Deutschland ist dafür das Datenschutz-Anpassungs- und Umsetzungsgesetz EU (DSAnpUG-EU) verabschiedet und im Juni 2017 im Bundesgesetzblatt verkündet worden.

Alle Unternehmen, die Produkte und Leistungen in der EU anbieten, unterliegen dieser Verordnung – die wichtigsten Informationen für Sie auf einen Blick.

maximum DSGVO im Detail



Datenschutz spielt überall eine Rolle – ob bei Kundenbestellungen, E-Mail-Kampagnen oder Nutzertracking. Für alle Unternehmer wie Shopbetreiber und Dienstleister ist Datenschutz schon immer ein wichtiges Thema gewesen. Ab dem 25. Mai 2018 kommen auf alle Unternehmen tiefgreifende Änderungen zu. Denn ab diesem Zeitpunkt gilt die neue EU-Datenschutz-Grundverordnung (EU-DSGVO) auch in Deutschland und das Datenschutzrecht wird in allen EU-Mitgliedsstaaten einheitlich und unmittelbar geregelt.

Die derzeit noch geltende Datenschutzrichtlinie 95/46/EG wird durch die Verordnung abgelöst, das Bundesdatenschutzgesetz (BDSG) sowie alle anderen nationalen Regelungen zum Datenschutz werden weitgehend verdrängt, bzw. das BDSG wird zeitgleich neu gefasst.

In vielen – vor allem kleineren – Unternehmen herrscht noch der Gedanke vor „das betrifft uns nicht, da sind wir zu klein“. Betrachtet man die Verordnung, wird schnell klar, dass dies nicht so ist.

Sowie Sie in eigenem oder fremdem Namen Dienstleistungen oder Waren in Deutschland oder der EU anbieten oder Mitarbeiter beschäftigen, kommt diese Verordnung für Sie zur Anwendung. Grundsätzlich geht es in der Verordnung um personenbezogene Daten. Auch wenn Sie nicht für Privatkunden tätig sind, werden Sie sicher Namen von Ansprechpartnern und somit personenbezogene Daten speichern. Die Verordnung bezieht sich dabei auf die Verarbeitung dieser personenbezogenen Daten. Verarbeitung im Sinne der Verordnung ist dabei:



Daten beschaffen
(ein Gewinnspiel auf einer Messe?)

Daten speichern
(Daten in der Software eintragen?)

Daten ändern
(eine Adresse aktualisieren?)

Daten nutzen
(nach einem Namen suchen?)

Daten übermitteln
(eine Visitenkarte weitergeben?)

Daten verknüpfen
(Ansprechpartner einem Unternehmen zuordnen?)

Daten löschen
(den Datensatz löschen?)

Egal was Sie tun – aus der DSGVO kommen Sie nicht raus.

Hieraus resultiert die Notwendigkeit, alle Verfahren, mit denen personenbezogene Daten verarbeitet werden, daraufhin zu überprüfen, ob es einen Anpassungsbedarf im Hinblick auf die DSGVO gibt. Wir informieren Sie hier im Detail.

Welche Ziele verfolgt die DSGVO?

Bisher gelten in Europa überall verschiedene Datenschutzgesetze und unterschiedliche Standards. Das primäre Ziel der DSGVO ist zunächst die Harmonisierung des unübersichtlichen Datenschutzrechts der einzelnen EU-Mitgliedsstaaten zu einem einheitlichen Datenschutzstandard. Sobald Unternehmen mit Sitz außerhalb der EU Daten von Personen aus der EU verarbeiten, gilt die DSGVO ebenfalls. Dadurch soll gewährleistet werden, dass sich auch Cloud-Dienste oder soziale Netzwerke z.B. aus den USA an die Verordnung halten müssen. Die DSGVO soll außerdem für gleiche

wirtschaftliche Rahmenbedingungen in der EU sorgen. Die einheitliche datenschutzrechtliche Basis soll auf lange Sicht auch zur Stärkung des Binnenmarktes führen. Des Weiteren soll der Datenschutz in Europa hinsichtlich der wachsenden Herausforderungen durch Cloud-Computing, Big Data, soziale Medien und Suchmaschinen modernisiert werden. Im Mittelpunkt steht dabei der Grundrechtsschutz des Einzelnen. Angesichts der vielfältigen neuen technischen Anwendungen ist diese Umgestaltung dringend erforderlich. Sie soll den Schutz natürlicher Personen und den freien Verkehr gewährleisten.

Wen betrifft die DSGVO?

„... die DSGVO ist doch nur für riesige Unternehmen und Shops mit großem Kundenstamm relevant“ – solche und ähnliche Meinungen schienen lange Zeit verbreitet zu sein. Tatsächlich ist es jedoch so, dass die DSGVO jedes Unternehmen betrifft, das in der EU ansässig ist oder das in irgendeiner Form personenbezogene Daten natürlicher Personen speichert.

Da darunter auch die eigenen Mitarbeiterdaten, z.B. für die Gehaltsabrechnung, fallen, ist quasi jedes Unternehmen betroffen.

Außereuropäische Unternehmen müssen sich dann an die DSGVO halten, wenn sie eine Niederlassung in der EU haben oder personenbezogene Daten von EU-Bürgern verarbeiten.

Kundendaten, Kontaktformulare auf Webseiten, Werbemails oder Newsletter, Werbung auf Facebook, Nutzertracking, die eigene Datenschutzerklärung: Vieles ändert sich durch die neue Verordnung.

Grundsätzlich geht es in der Verordnung um personenbezogene Daten. Das sind alle Informationen, die sich auf eine identifizierte oder identifizierbare Person beziehen. Eine Person gilt dann als „identifizierbar“, wenn sie indirekt oder direkt mittels Zuordnung zu einer Kennung wie Name, Kennnummer, Standortdaten u.a. identifiziert werden kann. Dabei reicht es aus, wenn allein die Möglichkeit besteht, die Person zu identifizieren.



Personenbezogene Daten sind:

Name, Adresse, E-Mail-Adresse, Telefonnummer, Geburtstag, Kontodaten, KfZ-Kennzeichen, Standortdaten, IP-Adressen, Cookies etc.

Den wichtigsten Anknüpfungspunkt beim Anwendungsbereich der DSGVO bildet die Verarbeitung der personenbezogenen Daten. Darunter fallen: Datenbeschaffung, Datenspeicherung, Datenänderung, Datennutzung, Datenübermittlung, Datenverknüpfung und Datenlöschung. Dafür wurde eine Vielzahl von allgemeinen Grundsätzen festgelegt, die jeder Verantwortliche einhalten und nachweisen können muss.

Unternehmen aller Art sollten im Hinblick auf die DSGVO alle Verfahren, die mit personenbezogenen Daten verarbeitet werden, dahingehend überprüfen, ob es einen Anpassungsbedarf gibt.

Verantwortlich für die Einhaltung der Regelungen ist immer der Geschäftsführer oder Unternehmer selbst – auch wenn ein Datenschutzbeauftragter eingestellt wurde.

Grundsätze der Datenverarbeitung

Rechtmäßigkeit der Verarbeitung

(Art. 5 (1) a) DSGVO):

Personenbezogene Daten müssen mit Einwilligung der betroffenen Person oder auf einer sonstigen zulässigen Rechtsgrundlage verarbeitet werden. Die Verarbeitung ist nur dann rechtmäßig, wenn mindestens eine der nachstehenden Bedingungen erfüllt ist:

- **Einwilligung** der betroffenen Person zur Verarbeitung ihrer Daten für einen oder mehrere bestimmte Zwecke. Die Einwilligung muss freiwillig erfolgen, für einen klar definierten Fall abgegeben sein und eine präzise Information beinhalten (wer braucht die Daten für welchen Zweck?).
- **Erfüllung eines Vertrags**, dessen Vertragspartei die betroffene Person ist. Durchführung vorver-

traglicher Maßnahmen, die auf Antrag der betroffenen Person erfolgen

- **Erfüllung einer rechtlichen Verpflichtung**, der der Verantwortliche unterliegt
- **Schutz lebenswichtiger Interessen** der betroffenen Person oder einer anderen natürlichen Person
- **Wahrnehmung einer Aufgabe**, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt
- **Wahrung berechtigter Interessen des Verantwortlichen oder eines Dritten** – sofern nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person, die den Schutz personenbezogener Daten erfordern, betroffen sind (besonders wenn es sich um ein Kind handelt)

Verarbeitung nach Treu und Glauben

(Art. 5 (1) a) DSGVO):

Rechtlich schwerer zu fassen und bisher nur am konkreten Einzelfall unter Berücksichtigung aller Umstände zu beurteilen. Meist geht es um die Frage, ob ein bestimmtes Verhalten als anständig oder redlich angesehen werden kann. Hier wird die Erfahrung zeigen, wie genau dieser Grundsatz zu handhaben ist.

Transparenz

(Art. 5 (1) a) DSGVO):

Stichwort „informationelle Selbstbestimmung“. Alle Informationen und Mitteilungen zur Verarbeitung dieser personenbezogenen Daten müssen leicht zugänglich, verständlich und in klarer und einfacher Sprache verfasst sein. Das betrifft insbesondere die Informationen zur Identität des Verant-

wortlichen und zu den Zwecken der Verarbeitung sowie andere Informationen, die eine faire und transparente Verarbeitung für die betroffenen Personen gewährleisten. Des Weiteren sollten die Personen über Risiken, Vorschriften, Garantien und Rechte im Zusammenhang mit der Verarbeitung ihrer Daten informiert und aufgeklärt werden, wie sie ihre diesbezüglichen Rechte geltend machen können.

Zweckbindung

(Art. 5 (1) b) DSGVO):

Die Speicherung, Nutzung und Verarbeitung von personenbezogenen Daten muss immer in Abhängigkeit von einem bestimmten Zweck gesetzt werden. Nach Erfüllung des Zwecks dürfen die Daten nicht mehr weiterverwendet werden. Sofern die Zwecke der Weiterverarbei-



tung mit den ursprünglichen Erhebungszwecken nicht unvereinbar sind und eine Rechtsgrundlage dafür vorliegt, ist eine Weiterverarbeitung zu anderen Zwecken möglich. Dafür stellt die DSGVO in Artikel 5 Kriterien auf, die bei der Beurteilung der Vereinbarkeit einer Zweckänderung berücksichtigt werden müssen:

- Verbindung zwischen den Zwecken
- der Gesamtkontext, in dem die Daten erhoben wurden
- die Art der personenbezogenen Daten
- mögliche Konsequenzen der zweckändernden Verarbeitung für den Betroffenen
- das Vorhandensein von angemessenen Sicherheitsmaßnahmen wie eine Pseudonymisierung oder Verschlüsselung der Daten

Datenminimierung (Art. 5 (1) c) DSGVO):

Personenbezogene Daten müssen dem Zweck angemessen und erheblich auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein.

Richtigkeit der Datenverarbeitung (Art. 5 (1) d) DSGVO):

Personenbezogene Daten müssen sachlich richtig und erforderlichenfalls auf dem neuesten Stand sein. Personenbezogene Daten, die hinsichtlich der Zwecke ihrer Verarbeitung unrichtig sind, müssen umgehend gelöscht oder berichtigt werden.

Speicherbegrenzung (Art. 5 (1) e) DSGVO):

Die personenbezogenen Daten dürfen lediglich in einer Form gespeichert werden, die die Identifizierung der Person nur so lange ermöglicht, wie es für die Zwecke der Verarbeitung erforderlich ist. Sobald die Speicherung der personenbezogenen Daten für den Verwendungszweck nicht mehr erforderlich ist, müssen sie gelöscht oder die Identifizierung der betroffenen Person aufgehoben werden. Ausnahmen: Archivzwecke von öffentlichem Interesse, wissenschaftliche oder historische Forschungszwecke und statistische Zwecke.

Integrität und Vertraulichkeit (Art. 5 (1) f) DSGVO):

Die Verarbeitung der personenbezogenen Daten muss immer eine angemessene

Sicherheit gewährleisten einschließlich dem Schutz vor unbefugter oder unrechtmäßiger Verarbeitung und vor unbeabsichtigtem Verlust oder versehentlicher Schädigung durch technische und organisatorische Maßnahmen.

Das droht bei Verstoß

Bei Verstoß gegen die Grundsätze der personenbezogenen Datenverarbeitung kann ein Bußgeld von bis zu 20 Millionen Euro erhoben werden. Im Falle eines Unternehmens kann der Verstoß bis zu 4 Prozent des gesamten weltweit erzielten Jahresumsatzes des vorangegangenen Geschäftsjahres und Maßnahmen der Aufsichtsbehörde nach sich ziehen. Der höhere Betrag bestimmt das Straf- bzw. Bußgeldmaß.

Was zählt als ein Verstoß gegen die DSGVO?

Eine Verletzung des Schutzes personenbezogener Daten liegt dann vor, wenn die Sicherheit – egal ob unbeabsichtigt (z.B. durch ein technisches Problem) oder unrechtmäßig (z.B. durch einen Hacker) – verletzt wurde und Folgendes nach sich zieht:

- **Datenverlust:** Personenbezogene Daten wurden



- zerstört oder befinden sich nicht mehr im Zugriff des Verantwortlichen
- **Unrichtige Veränderung der Daten:** Personenbezogene Daten sind nicht mehr korrekt bzw. unzuverlässig
- **Unbefugte Offenlegung der personenbezogenen Daten:** Jemand könnte Zugriff erhalten
- **Unbefugter Zugang zu den personenbezogenen Daten:** Jemand hat Zugriff erhalten

Es liegt bereits dann eine Verletzung des Schutzes der personenbezogenen Daten vor, wenn allein die Möglichkeit einer Verletzung gegeben ist. Es muss nicht erst ein messbarer Schaden entstanden sein!

Was tun bei Verletzung des Schutzes personenbezogener Daten?

Wenn es zu einer Verletzung im Sinne der DSGVO kommt, dann ist in jedem Fall „unverzüglich“ innerhalb von 72 Stunden ...

- ... die zuständige Aufsichtsbehörde (gemäß Artikel 55) zu benachrichtigen. Die Meldepflicht besteht, sobald die Verletzung bekannt ist.
- ... die betroffenen Personen zu informieren (im Falle eines hohen Risikos für die „Rechte und Freiheiten“ der betroffenen Personen).

Die Meldung muss (gemäß Absatz 1) folgende Informationen beinhalten:

- **Beschreibung der Art der Verletzung** des Schutzes

personenbezogener Daten, Angabe der Kategorien und der ungefähren Zahl der betroffenen Personen, der betroffenen Kategorien und der ungefähren Zahl der betroffenen personenbezogenen Datensätze

- **Name und Daten des Datenschutzbeauftragten** oder einer sonstigen Anlaufstelle für weitere Informationen
- **Beschreibung der wahrscheinlichen Folgen** der Verletzung des Schutzes personenbezogener Daten
- **Beschreibung der von dem Verantwortlichen ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung** der Verletzung des Schutzes personenbezogener Daten und gegebenenfalls Maß-

nahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen

Falls nicht alle Informationen gleichzeitig zur Verfügung gestellt werden können, hat der Verantwortliche die Möglichkeit, diese ohne unangemessene weitere Verzögerung schrittweise bereitzustellen. Der Verantwortliche dokumentiert Verletzungen des Schutzes personenbezogener Daten einschließlich aller im Zusammenhang mit der Verletzung des Schutzes personenbezogener Daten stehenden Fakten, deren Auswirkungen und der ergriffenen Abhilfemaßnahmen. Diese Dokumentation ermöglicht der Aufsichtsbehörde die Überprüfung der Einhaltung der Bestimmungen dieses Artikels.

Betroffenenrechte

Zum Großteil sind die Rechte der betroffenen Personen bereits im BDSG vermerkt. Der Schutz der betroffenen Personen ist eines der Hauptanliegen der DSGVO. Daher sollen diese Rechte gestärkt und präzisiert werden. Aufgrund der erheblich höheren Sanktionen sind Verantwortliche unbedingt dazu angehalten, den Rechten auch nachzukommen. Formulare

und Prozesse müssen rechtzeitig angepasst werden. Die DSGVO kennt die folgenden „Rechte der betroffenen Person“:



- Informationsrecht
- Auskunftsrecht
- Recht auf Datenübertragbarkeit
- Recht auf Berichtigung
- Recht auf Löschung/ Vergessenwerden
- Recht auf Einschränkung der Verarbeitung
- Widerspruchsrecht

Im Folgenden werden die Rechte noch einmal etwas ausführlicher betrachtet.

Informationsrecht

Ab Mai 2018 sind die betroffenen Personen über sämtliche Umstände der Datenverarbeitung bei dem Verantwortlichen zu informieren. Die Verantwortlichen haben Informationspflicht bei der Erhebung von personenbezogenen Daten gegenüber den betroffenen Personen – oder wenn die personenbezogenen Daten nicht bei der betroffenen Person erhoben wurden. Pflichtangaben sind:

- Kontaktdaten des Verantwortlichen und des Datenschutzbeauftragten
- Zwecke der Datenverarbeitung
- Speicherdauer der Daten
- Betroffenenrecht

Der Verantwortliche muss der betroffenen Person alle Informationen nach dem Grundsatz der Transparenz übermitteln.

Auskunftsrecht

Die betroffene Person ist berechtigt zu erfragen, ob und ggf. welche Daten über sie gespeichert sind. Neu ist, dass der Verantwortliche auch darüber informieren muss, wie lange seine Daten gespeichert werden bzw. welche Kriterien zur Bestimmung der Datenspeicherungsfrist herangezogen werden. Der Verantwortliche muss außerdem Auskunft über die Rechte auf Berichtigung, Löschung oder Einschränkung der Verarbeitung sowie das Beschwerderecht bei der Aufsichtsbehörde erteilen. Innerhalb eines Monats muss der betroffenen Person die erste Kopie der Auskunft (Überprüfung auf Vollständigkeit der Angaben und ggf. Anpassung) unentgeltlich zugestellt werden.

gotomaxx Onlineseminar

DSGVO-Grundlagen

Ist mein Unternehmen betroffen?
Wer ist verantwortlich?
Mit welchen Aktivitäten starte ich?

Wir geben einen kurzen Einblick in den Inhalt der DSGVO und klären die wichtigsten Begrifflichkeiten.

09.04.2018 & 13.04.2018



Anmelden und weitere Informationen:

www.gotomaxx.de/dsgvo

Recht auf Datenübertragbarkeit

Dieses Recht ist neu und erlaubt betroffenen Personen unter bestimmten Voraussetzungen, eine Kopie der sie betreffenden personenbezogenen Daten in einem üblichen und maschinenlesbaren Dateiformat zu erhalten. Auf diese Weise kann der Nutzer seine Daten von einem Anbieter zu einem anderen „portieren“. Das gilt allerdings nur für die Daten, die die betroffene Person selbst zur Verfügung gestellt hat.

Bis Mai 2018 müssen Verantwortliche einen Prozess entwickelt haben, mit dem sie dieses Recht der betroffenen Personen bedienen können.

Vor allem im Endkundenbereich könnten bereits Ende Mai 2018 erste Herausforderungen bei den Unternehmen eintreffen.

Recht auf Berichtigung

Falsche personenbezogene Daten müssen von dem Verantwortlichen unverzüglich berichtigt sowie unvollständige Daten vervollständigt werden. Die Gewährleistung dieses Rechts liegt regelmäßig im Interesse des Verant-

wortlichen, da nur die Verarbeitung richtiger Daten der Zweckerreichung dient.

Recht auf Löschen/Vergessenwerden

Die betroffene Person hat das Recht auf das Löschen ihrer personenbezogenen Daten, wenn die Notwendigkeit der Datenverarbeitung nicht mehr gegeben ist – also entweder bei Erreichen oder Wegfall des Zwecks.

Ein Antrag auf Löschung kann trotz Vorliegen eines Löschrgrundes rechtmäßig abgelehnt werden, wenn der Verantwortliche ein berechtigtes Interesse (z.B. Befolgung gesetzlicher Aufbewahrungspflichten oder Ausübung von Rechtsansprüchen) an der Weiternutzung der Daten hat. Wurden die zu löschenden Daten an Dritte weitergegeben oder sogar öffentlich gemacht, muss der Verantwortliche bei Vorliegen eines Löschrgrundes alle Dritten (sofern möglich) über die Löschung informieren, damit auch diese die Löschungsvorgänge einleiten können. Möchte die betroffene Person eine Auskunft über die Drittpersonen haben, muss ihm diese unverzüglich erteilt werden. Die Löschrpflichten sind mit erhöhten Sanktionen belegt.

Recht auf Einschränkung und Verarbeitung

Diesem Recht ist nur dann nachzukommen, wenn die betroffene Person es verlangt. Bei Einschränkung darf der Verantwortliche bis zur Aufhebung die gespeicherten Daten nur eingeschränkt nutzen. Die betroffene Person muss nach Aufhebung der Einschränkung durch den Verantwortlichen informiert werden. Der Verantwortliche ist im Falle der Einschränkung zusätzlich verpflichtet (sofern möglich), Dritte, an die die Daten übermittelt wurden, zu informieren, damit diese ihre Verarbeitungsprozesse selbst einschränken können.

Widerspruchsrecht

Auch bei einer an sich rechtmäßigen Verarbeitung ihrer Daten haben betroffene Personen aus Gründen, die sich aus ihrer besonderen Situation ergeben, ein Widerspruchsrecht. Die Daten dürfen nur noch dann verarbeitet werden, wenn zwingende berechnete Gründe für die Verarbeitung nachweisbar sind, „die die Interessen, Rechte und Freiheiten der betroffenen Person überwiegen“. Liegt kein zwingender Grund vor, die personenbezogenen Daten weiter zu verarbeiten,

dürfen sie nach Widerspruch mit sofortiger Wirkung nicht mehr genutzt werden.

Die betroffene Person ist nach dem Grundsatz der Transparenz und getrennt von jeglicher anderer Information in jedem Fall auf das bestehende Widerspruchsrecht hinzuweisen.

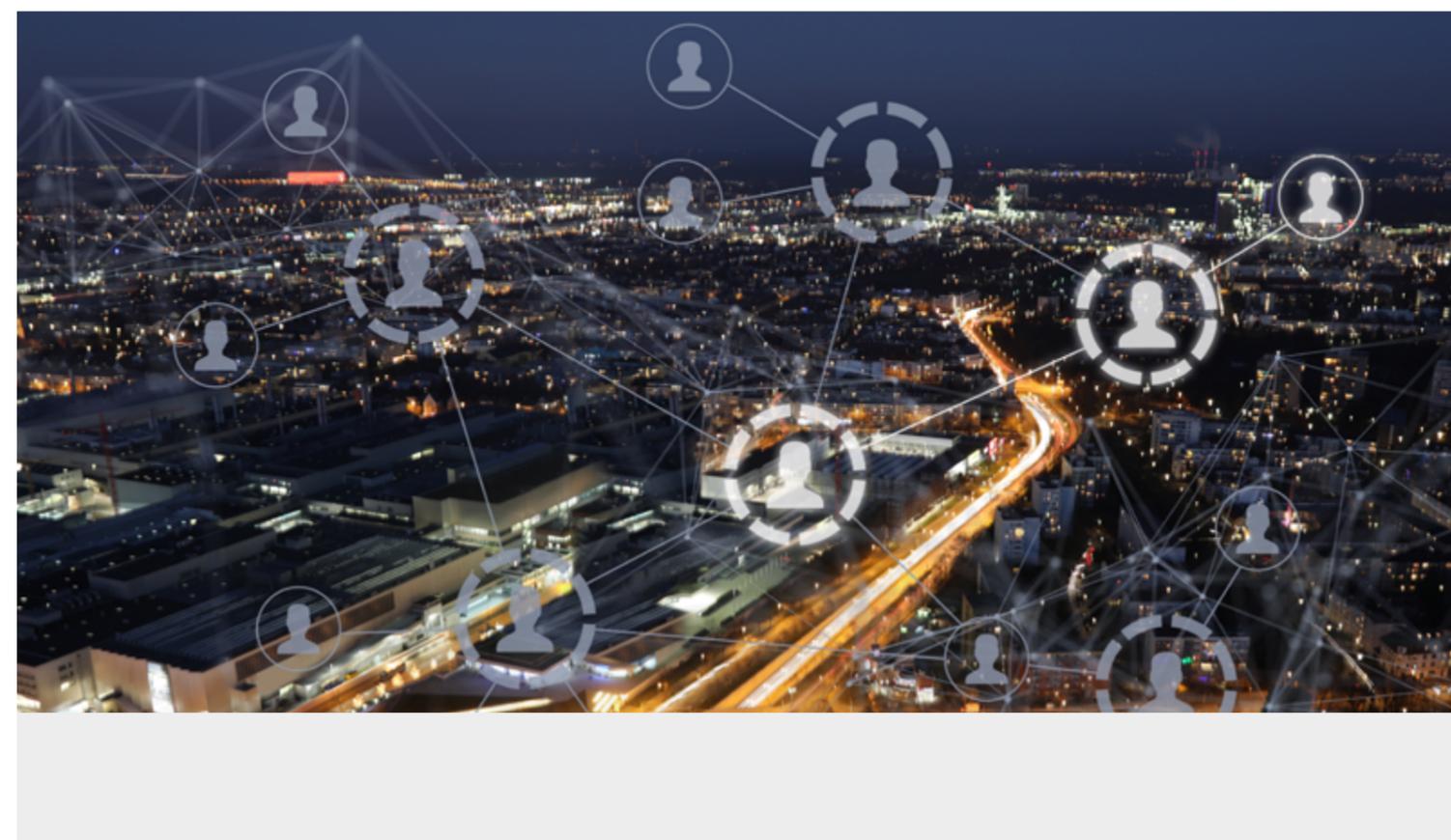
Wo liegen die Unterschiede zur bisherigen Rechtslage im BDSG?

Einige Betroffenenrechte (Recht auf Auskunft, Berich-

tigung, Löschung [Vergessenwerden] und Sperrung) sind auch im BDSG geregelt. Allerdings sind die Anforderungen an Inhalt und Form der Informationsrechte des Betroffenen in der DSGVO viel strenger ausgearbeitet. Dadurch ist die Wahrscheinlichkeit bußgeldbewehrter Verstöße sehr hoch. Das Recht auf Datenübertragbarkeit ist eine Neuerung im Rahmen der DSGVO.

Neu ist auch, dass die Verordnung alle Unternehmen

einbezieht, die personenbezogene Daten von EU-Bürgern verarbeiten – unabhängig vom tatsächlichen Sitz des Unternehmens.



FAZIT

Die DSGVO steht in ihren Startlöchern. Ab 25. Mai 2018 ist sie Pflicht für alle Unternehmen, die in der EU ansässig sind oder die in irgendeiner Form personenbezogene Daten natürlicher Personen speichern.

Das bedeutet für die Verantwortlichen eine zeitnahe Einrichtung bzw. Anpassung von Prozessen, IT-Systemen und Strukturen der Datenverarbeitung unter Berücksichtigung der geänderten gesetzlichen Vorgaben, auch um den erheblich verschärften Bußgeld- und Haftungsrisiken zu begegnen.

JETZT HANDELN – auch auf der Webseite



Die neue DSGVO klingt aufgrund der hohen Bußgelder zunächst bedrohlich, aber im Detail schafft sie auch einen einheitlichen Raum innerhalb der Mitgliedsstaaten der EU. Einige Punkte erfordern zunächst Mehraufwand, aber an anderer Stelle hat es auch Vereinfachungen gegeben.

Für Unternehmen ist es entscheidend, jetzt zu handeln, und Sie sind bestens gerüstet, wenn am 25. Mai 2018 die Schonfrist endet.

Hier noch einmal die wichtigsten „To-dos“ im Überblick:



- ✓ **1. Bestandsaufnahme**
Welche personenbezogenen Daten werden in Ihrem Unternehmen verarbeitet?
- ✓ **2. Prozesse dokumentieren**
Legen Sie ein Verzeichnis für Verarbeitungstätigkeiten an, in dem alle Geschäftsabläufe dokumentiert sind, bei denen personenbezogene Daten verarbeitet werden. Aktualisieren Sie es regelmäßig.
- ✓ **3. Datenschutzerklärung anpassen**
Evaluieren Sie Ihre Rechtsgrundlage für die Verarbeitung von personenbezogenen Daten und geben Sie diese in Ihrer Datenschutzerklärung an.
- ✓ **4. Prozesse gestalten**
Gewährleisten Sie, dass Sie die 72 Stunden Meldefrist bei einer Datenschutzverletzung einhalten können.
- ✓ **5. Weitere Prozesse gestalten**
Überprüfen Sie die Datenerfassungsprozesse und passen Sie diese wenn nötig an. Kontrollieren Sie, ob Ihre bisher erfassten Daten die Mindestnormen für die Einwilligung erfüllen.
- ✓ **6. Kontrollieren Sie Ihre Datenschutzverfahren,**
um sicher zu sein, dass Sie allen erweiterten Rechten von Einzelpersonen nachkommen können.
- ✓ Nutzen Sie für die Einwilligung der Betroffenen: Checkboxen und Double-Opt-in.
- ✓ Kommen Sie Ihrer Informationspflicht nach und aktualisieren Sie sämtliche Rechtstexte wie Einwilligungstexte, Datenschutzinformationen, ggf. AGBs oder sonstige Informationstexte.
- ✓ Berücksichtigen Sie dabei auch Ihre Hinweispflicht auf das Widerrufsrecht.
- ✓ Treffen Sie Vorkehrungen in Bezug auf die Dokumentationspflicht.
- ✓ Legen Sie ein Verzeichnis an.
- ✓ Passen Sie Ihre Auftragsdatenverarbeitungsverträge an.



Für wen die DSGVO gilt

- Für alle Unternehmen, die in der EU ansässig sind oder in irgendeiner Form personenbezogene Daten natürlicher Personen speichern
- Auch für Anbieter außerhalb der EU, wenn sie ihre Angebote an Bürger in der EU richten (wie etwa Facebook und Google)
- Der Ort der Datenverarbeitung spielt keine Rolle mehr



Die Ziele der DSGVO

- Vereinheitlichung des Datenschutzrechts in allen EU-Mitgliedsstaaten
- Gleichheit wirtschaftlicher Rahmenbedingungen in der EU und somit auf langfristige Sicht Stärkung des Binnenmarktes
- Gewährleistung des Schutzes natürlicher Personen



Datenschutzverstöße

- Alle Datenschutz-Pannen müssen gemeldet werden, sofern ein Datenschutzrisiko besteht
- Die Meldung muss innerhalb von 72 Stunden nach Kenntnis bei der Aufsichtsbehörde erfolgen



Bußgelder

- Fast jeder Verstoß gegen die DSGVO kann geahndet werden!
- Der Bußgeldrahmen wird deutlich erhöht und kann bis zu 20 Mio. EUR oder 4 Prozent des gesamten weltweit erzielten Jahresumsatzes betragen (je nachdem, welcher Betrag höher ist)



Informationsrechte

- Betroffene müssen umfangreicher als bisher über die Datenverarbeitung und über ihre Rechte informiert werden – z.B. Angaben über Speicherdauer und Kontaktdaten des Datenschutzbeauftragten
- Bei Heranziehen der Interessensabwägung als Rechtsgrundlage müssen auch die „berechtigten Interessen“ aufgezählt werden



Privacy by design and default

- Datenschutz muss bereits beim Planen neuer Techniken und neuer Verarbeitungen sowie durch datenschutzfreundliche Grundeinstellungen berücksichtigt werden



Transparenz

- Stichwort „informationelle Selbstbestimmung“
- Alle Informationen und Mitteilungen zur Verarbeitung dieser personenbezogenen Daten müssen leicht zugänglich und verständlich und in klarer und einfacher Sprache verfasst sein
- Vor allem bei Informationen über die Identität des Verantwortlichen und die Zwecke der Verarbeitung gilt dieser Grundsatz
- Personen sollen über Risiken, Vorschriften, Garantien und Rechte im Zusammenhang mit der Verarbeitung ihrer Daten informiert werden
- Personen müssen verpflichtend aufgeklärt werden, wie sie ihre diesbezüglichen Rechte geltend machen können



Briefe als Service

Komplett produziert und frankiert im Druckzentrum. Durch Outsourcing erzielen Sie Topkonditionen beim Postversand.



E-Mail und Bezahlen

Bieten Sie Empfängern eine Bezahlungsmöglichkeit direkt im E-Mail-Body, z.B. per PayPal oder Kreditkarte.



Elektronische Rechnung

Stellen Sie elektronische Rechnungen im PDF/A-Format inkl. ZUGFeRD-Daten bereit.



Rechnungsportal

Bieten Sie Kunden einen besseren Service durch ein Rechnungsportal mit Beleghistorie.



PDF + Bezahlen

Erhalten Sie mehr Aufträge und machen Sie mehr Umsatz. Nutzen Sie eine Bezahlungsfunktion in Angeboten mit „PDF-Payment“.



Campaign1to1

Realisieren Sie Marketingkampagnen per Brief – automatisiert und ohne Streuverluste.



Mitarbeiterportal

Automatisieren Sie die Verteilung von Lohn- und Gehaltsabrechnungen sowie Mitarbeiterinformationen.



Werbebelegger

Legen Sie Ihren Rechnungen Werbung bei. Steuern Sie Ihre Botschaft artikel- und kundengenau.



Neues von gotomaxx: PDFMAILER 6.1

Die Dokumente werden mithilfe des PDFMAILERs verschlüsselt und unter Verwendung einer zweistufigen Authentifizierung aufbewahrt. Sie erhalten das verschlüsselte Dokument in Ihrem PDFMAILER-Konto und den Authentifizierungsschlüssel per SMS. Bitte beachten Sie die für Sie vorgeschriebenen Löschungsvorschriften für diese Dokumente.

Rechtsanwalt Michael Menk,
Kuentzle Rechtsanwälte Partnerschaft mbB



maximum

Was haben PDFMAILER 6.1 und die Verschlüsselung von PDF-Dateien mit der DSGVO zu tun?

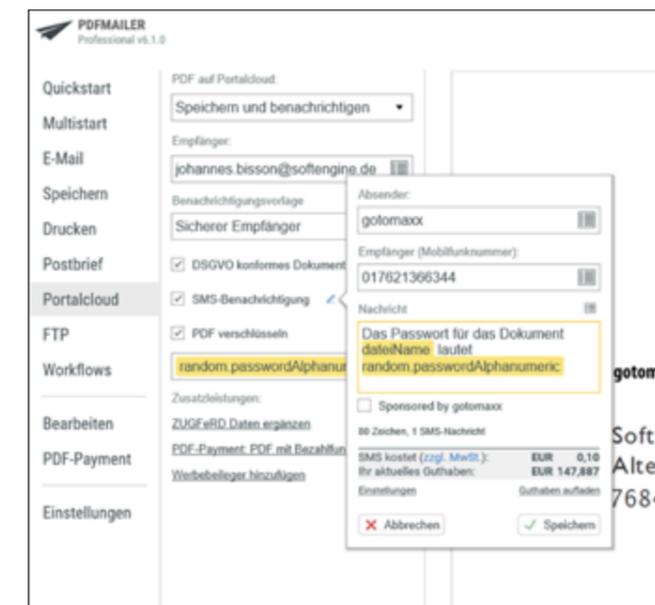
Übersichtlich, selbsterklärend, effizient – im März löst der PDFMAILER 6.1 seinen Vorgänger ab und überzeugt durch erweiterte Funktionen und Anwendungen, die auch hinsichtlich der EU-DSGVO von herausragender Bedeutung sind.

Eine Kernforderung der DSGVO ist die Verschlüsselung aller Dokumente, die personenbezogene Daten wie den Namen des Ansprechpartners und die E-Mail-Adresse des Empfängers/Absenders enthalten. Die Verschlüsselung soll Daten gezielt schützen, Datendiebe ausbremsen und den weitreichenden Folgen einer Datenpanne vorbeugen.

2017 wechselten insgesamt mehrere Milliarden Datensätze – fast alle unverschlüsselt gespeichert und damit sofort einsatzbereit – unfreiwillig den Besitzer. Vor diesem Hintergrund gewinnt die neue DSGVO noch mehr an Bedeutung. Sie nimmt Organisationen in die Pflicht, personenbezogene Daten angemessen zu schützen.

DSGVO-konforme Dokumente

Mit der Funktion „Verschlüsselung von PDF“ innerhalb des PDFMAILERS 6.1 stellt gotomaxx eine Funktion zur Verfügung, die es seinen Anwendern ermöglicht, DSGVO-konforme Dokumente zu erstellen. Das Dokument an sich wird zunächst durch einen PIN (zum Öffnen) gesichert und in einem weiteren Schritt durch die Verschlüsselung vor fremdem Zugriff geschützt.



NEUE Funktion: der SMS-Service

Der PIN zum Öffnen des Dokuments wird dem Anwender per SMS – also über einen autarken Kanal – zugeschickt.

Portalcloud garantiert vertrauliche Bereitstellung der PDF-Dokumente

Über die sichere Verbindung https wird das verschlüsselte Dokument in die gotomaxx Portalcloud gestellt. Der Anwender erhält eine E-Mail mit einem Link, der ihn direkt auf die Portalcloud weiterleitet.

2-Faktor-Authentifizierung bietet zusätzliche Sicherheit

Bevor sich die Portalcloud öffnet, muss sich der Anwender mit Benutzername und Passwort authentifizieren. Erst dann kann er das PDF-Dokument anklicken. Jetzt kommt der PIN zum Einsatz, der per SMS versendet wurde. Nach richtiger Eingabe öffnet sich das PDF-Dokument. Die Verschlüsselung wird in Artikel 32 zur Sicherheit der Verarbeitung personenbezogener Daten als „geeignete technische Maßnahme“ empfohlen und anerkannt. Eine gute Verschlüsselungslösung ist die letzte Barrikade, wenn Angreifer alle Hürden wie Firewall, Antivirensoftware oder weitere Sicherungslösungen genommen haben. Die Verschlüsselung verhindert, dass Datendiebe Profit aus den Informationen ziehen können. Mit verschlüsselten PDF-Dokumenten bleibt die Vertraulichkeit gewahrt.

PDFMAILER Professional v6.1.0

Rechnung.pdf

Quickstart
Multistart
E-Mail
Speichern
Drucken
Postbrief
Portalcloud
FTP
Workflows
Bearbeiten
PDF-Payment
Einstellungen

PDF auf Portalcloud:
Speichern und benachrichtigen

Empfänger:
johannes.bisson@softengine.de

Benachrichtigungsvorlage
Sicherer Empfänger

DSGVO konformes Dokument ?
 SMS-Benachrichtigung
 PDF verschlüsseln

Zusatzleistungen:
[ZUGFeRD Daten ergänzen](#)
[PDF-Payment: PDF mit Bezahlungsfunktion](#)
[Werbebeileger hinzufügen](#)

gotomaxx software gmbh | Alte Bundesstraße 16 | 76846 Hauenstein

SoftENGINE GmbH
Alte Bundesstraße 16
76846 Hauenstein

PDFMAILER Professional v6.1.0

Rechnung.pdf

Quickstart
Multistart
E-Mail
Speichern
Drucken
Postbrief
Portalcloud
FTP
Workflows
Bearbeiten
PDF-Payment
Einstellungen

PDF auf Portalcloud:
Speichern und benachrichtigen

Empfänger:
johannes.bisson@gotomaxx.de

Benachrichtigungsvorlage
Info

DSGVO konformes Dokument ?
 SMS-Benachrichtigung
 PDF verschlüsseln

Zusatzleistungen:
[ZUGFeRD Daten ergänzen](#)
[PDF-Payment: PDF mit Bezahlungsfunktion](#)
[Werbebeileger hinzufügen](#)

random passwordAlphanumeric

gotomaxx software gmbh | Alte Bundesstraße 16 | 76846 Hauenstein

SoftENGINE GmbH
Alte Bundesstraße 16
76846 Hauenstein

gotomaxx

gotomaxx software gmbh
Alte Bundesstraße 16
76846 Hauenstein
Telefon: (06392) 995100
Telefax: (06392) 995599
info@gotomaxx.com
www.gotomaxx.com
Geschäftsführer:
Dirk Winter, Matthias Neumer

RECHNUNG

Rechnungsnummer I2345AB
Bestellnummer B-I2345AB
Bestellt von Rita Birkenherz

Datum 16.02.2018

PDF auf Portalcloud: speichern und benachrichtigen, enthält eine Seite
Benötigtes Kontingent: 1

FAZIT

Der PDFMAILER 6.1 von gotomaxx schützt Dokumente, die personenbezogene Daten enthalten, bei allen Vorgängen wie Versand, Übermittlung, Bereitstellung und Aufbewahrung und wird damit den Anforderungen der DSGVO in vollem Umfang gerecht.



maximum

Interview mit Johannes Bisson

„Inwiefern bedeutet die DSGVO Neuerungen für gotomaxx Lösungen?“



Die EU-Datenschutz-Grundverordnung (EU-DSGVO) erhöht die Anforderungen an Datenschutz und Datensicherheit bei der Verarbeitung personenbezogener Daten. Bei Nichteinhaltung der Vorgaben drohen weitreichende Konsequenzen, vor allem hinsichtlich der drastisch erhöhten Bußgelder.

Johannes Bisson, Technical Consultant bei gotomaxx, erklärt, wie sein Unternehmen das Thema bewertet, wie die neuen Anforderungen umgesetzt werden und wo besondere Herausforderungen liegen.

➤ „Herr Bisson, warum ist die DSGVO für gotomaxx von Bedeutung?“

👤 Die gotomaxx Software bietet als Dienstleistung ein komplettes Output Management an, das unter anderem auch personenbezogene Daten enthält. Daher nehmen wir dieses Thema sehr

ernst, um unseren Kunden eine gesetzeskonforme und einwandfreie Dienstleistung und Softwarelösungen anbieten zu können.

Um die Sicherheit und den Schutz der personenbezogenen Daten zu gewährleisten, bedarf es einer intelligenten Zugangsregelung.

➤ Wie geht gotomaxx dieses Thema an oder was sind die herausragenden DSGVO-Implementierungen bei den gotomaxx Produkten?“

👤 Dieses Thema verfolgt uns schon einige Monate sehr intensiv. Zusammen mit unserem Datenschutzbeauftragten und unserer

„Um die Sicherheit und den Schutz der personenbezogenen Daten zu gewährleisten, bedarf es einer intelligenten Zugangsregelung.“

Rechtsabteilung passen wir unsere Prozesse an die neuesten Verordnungen und Gesetze an. Hier ist vor allem die neue Funktion „PDF verschlüsseln“ zu nennen, die im PDFMAILER 6.1 zu finden ist. Durch verschiedene Sicherungsmaßnahmen wie die 2-Faktor-Authentifizierung, Passwort-gesichertes PDF mit PIN, https-Up- und -Download in die Portalcloud und die SMS-Zustellung der PIN gewährleisten wir, dass ein PDF-Dokument absolut DSGVO-konform zu seinem rechtmäßigen Empfänger gelangt. Auch die Bereitstellung und Aufbewahrung des PDF-Dokuments entspricht damit den Anforderungen der DSGVO.

➤ „Wo sehen Sie persönlich die größten Herausforderungen?“

👤 Die Herausforderung liegt ganz klar im Umgang mit personenbezogenen Daten – sei es der Austausch, die Kommunikation oder auch die reine Speicherung. Eine Herausforderung ist, Kunden und Partnern, die mit unserer Software und Dienstleistung

arbeiten, Sicherheit zu geben sowie vollstes Vertrauen und Verlässlichkeit zu schaffen. Nicht zuletzt steht die neue DSGVO IT-Abteilung beim Managen von personenbezogenen Kundendaten vor großen Herausforderungen.

➤ „Und wie wird gotomaxx Partnern und Anwendern dieses Sicherheitsgefühl vermittelt? Gibt es zum Beispiel Informationsangebote, die sie nutzen können?“

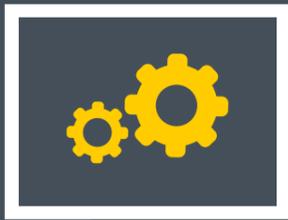
👤 Ja genau, unsere Kunden und Partner werden über sämtliche Kanäle informiert und stehen somit in einem Dialog mit uns. Beispielsweise bieten wir Endkunden-Seminare an, die sich mit aktuellen Themen beschäftigen, da gehört die DSGVO und alles, was damit zusammenhängt, natürlich auch dazu. Außerdem gibt es verschiedene Onlineschulungen, die viel genutzt werden und auch immer auf wichtige Fragestellungen aus der Kunden- und Partnerecke reagieren. Dann nutzen wir die ganz klassischen Kanäle wie Social Media und Newsletterversand. Ganz viel funktioniert

bei uns aber auch über den persönlichen oder telefonischen Kontakt zum Kunden über die Kundenbetreuung.

➤ „Haben Sie noch einen Rat für gotomaxx Partner und deren Anwender?“

👤 Ich würde unseren Kunden und Partnern empfehlen up to date zu sein, also unser vielfältiges Informationsangebot zu nutzen oder uns bei Unsicherheiten persönlich zu kontaktieren. Wichtig ist auch, dass man immer mit den neuesten Versionen arbeitet, denn dann ist gewährleistet, dass alle Funktionen und Features den aktuellen Anforderungen der DSGVO entsprechen. Ich denke, wenn man diese beiden Grundsätze ernst nimmt, ist man auf jeden Fall schon mal auf der sicheren Seite.

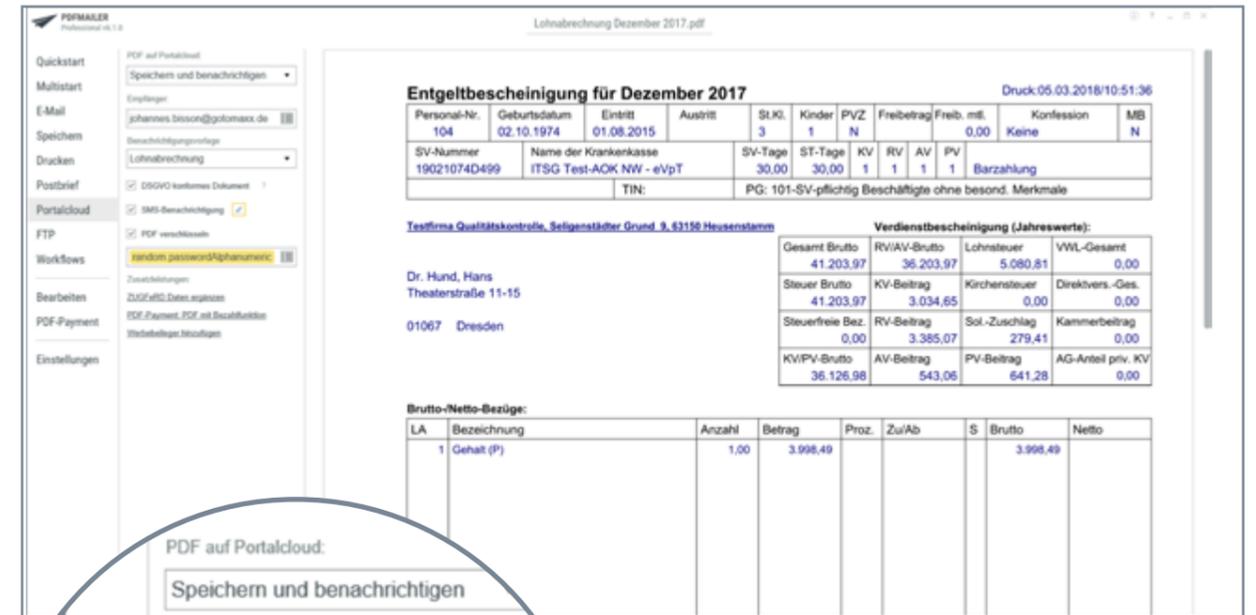
➤ „Das klingt logisch. Dann schauen wir mal ganz entspannt auf den 25. Mai. Vielen Dank für das Gespräch, Herr Bisson.“



maximum

Workshop:

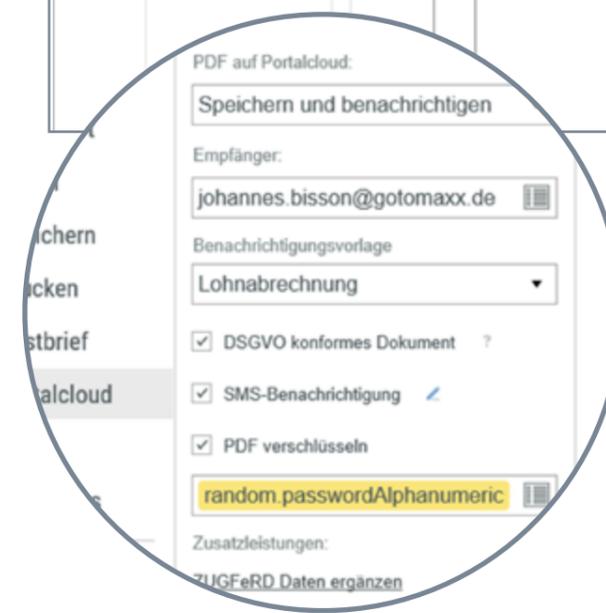
Verschlüsselung von PDF-Lohnabrechnungen mit PDFMAILER 6.1



Das mit Abstand wichtigste Feature des PDFMAILERs 6.1 hinsichtlich der DSGVO ist die Verschlüsselung von PDF-Dateien. Mit dieser Funktion wird die gotomaxx Software den Anforderungen der neuen Datenschutzvorgaben gerecht und kann Compliance-Regeln in einem überschaubaren Rahmen einhalten.

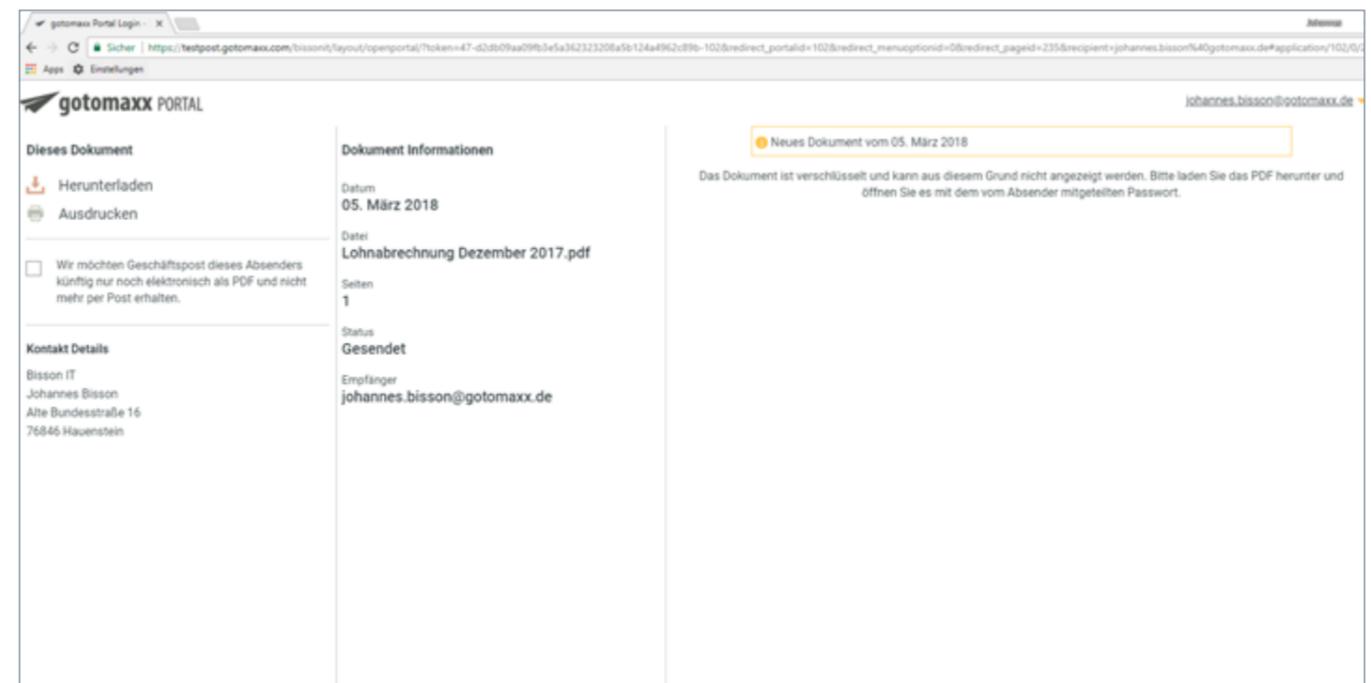
Unser kleiner Workshop zeigt Ihnen, wie die Verschlüsselung mit dem PDFMAILER 6.1 funktioniert.

- 1 Erstellen Sie die Lohnabrechnung in Ihrer SoftENGINE ERP.
- 2 Gehen Sie nun auf „Drucken“ und wählen Sie den PDFMAILER 6.1 aus.
- 3 Der PDFMAILER öffnet sich. Klicken Sie auf „Portalcloud“ und haken Sie den Punkt „DSGVO konformes Dokument“ an. Alle Einstellungen, die dazu nötig sind (PDF-Verschlüsselung, SMS Benachrichtigung, PIN zum Öffnen des Dokuments), werden automatisch vorausgefüllt. Wählen Sie noch eine Zustellart aus, und geben Sie eine E-Mail-Adresse an.



- 4 Der Workflow muss die folgenden Punkte enthalten:
 - a) DSGVO-konformes Dokument
 - b) SMS-Versand der PIN an Benutzer
 - c) PDF-Verschlüsselung

- 5 Das Dokument wird per https in die gotomaxx Portalcloud hochgeladen.

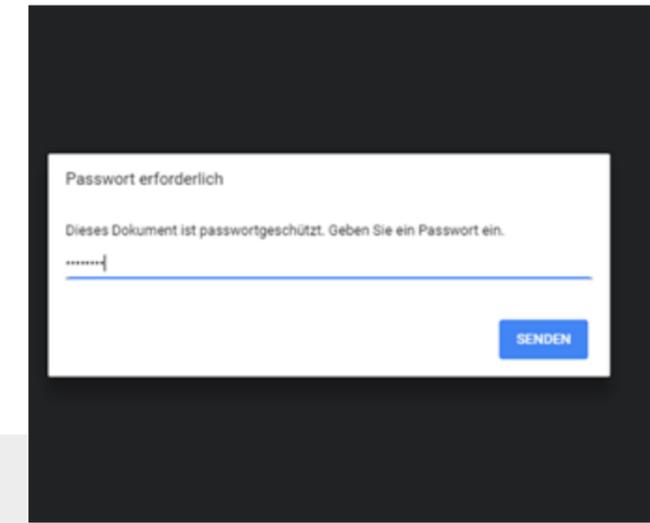
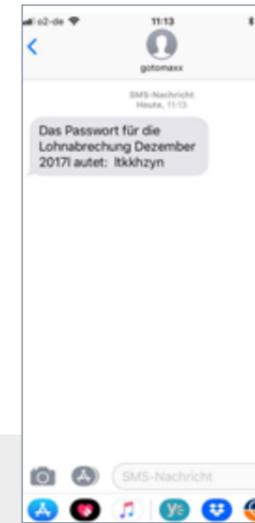


- 6 Der Empfänger wird per E-Mail benachrichtigt, dass ein neues Dokument in der Portalcloud für ihn bereitliegt.

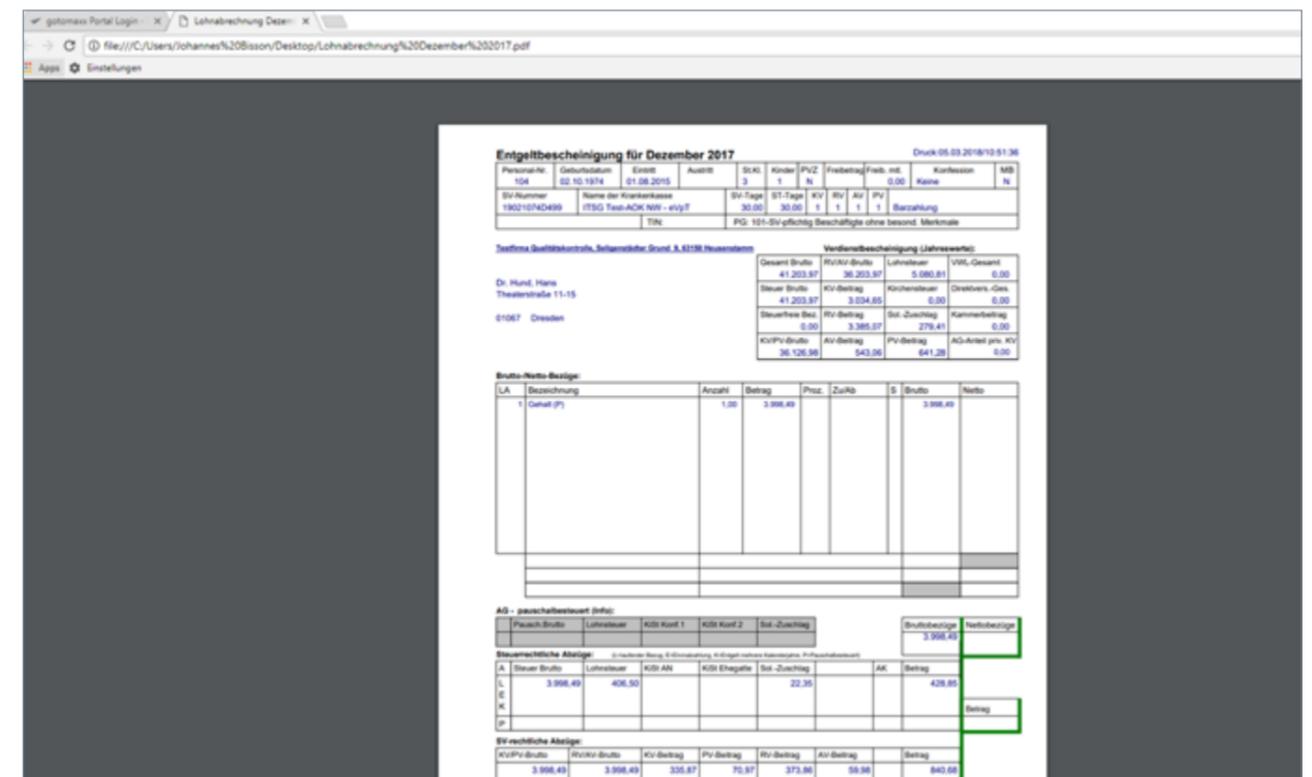


- 7 Der Empfänger muss nur auf den Link in der E-Mail klicken und die sichere https-Verbindung öffnet sich.

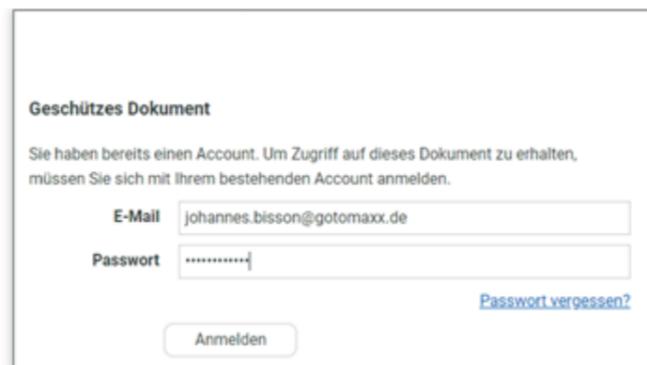
- 9 Anschließend erscheint ein Feld, in dem der E-Mail-Empfänger die per SMS erhaltene PIN eintragen muss.



- 10 Das Dokument öffnet sich.



- 8 Authentifizierung des Empfängers durch Benutzername und Passwort.



FAZIT

In gewohnt zeitsparender und selbsterklärender Weise liefert der PDFMAILER – hier in der neuen Version 6.1 – einen wichtigen Beitrag zur Gewährleistung einer DSGVO-konformen Anwendung. So sind Sie als Partner und Anwender immer auf der sicheren Seite, wenn es darum geht, Dateien mit personenbezogenen Daten zu versenden, bereitzustellen oder aufzubewahren.



XRechnung und ZUGFeRD 2.0 – die elektronischen Rechnungsformate für die öffentliche Verwaltung

Ab November 2018 verpflichtet die EU-Richtlinie 2015/55/EU alle öffentlichen Auftraggeber zum Empfang und zur Verarbeitung elektronischer Rechnungen. Das Datenaustauschformat XRechnung/ZUGFeRD 2.0 wird als Standard für elektronische Rechnungen eingeführt und ist die Bezeichnung für einen einheitlichen internen Rechnungsbegriff.



maximum

Zukunftsorientiert und EU-konform – PDFMAILER 6.1

Das XRechnungs-Format reiht sich ein in die Familie der XÖV-Standards. XÖV steht dabei für „XML in der öffentlichen Verwaltung“. Zuerst wird das neue elektronische Rechnungsformat für Bundesministerien und Verfassungsorgane verpflichtend, nämlich ab dem 27. November 2018. Alle anderen Bundesstellen müssen das digitale Rechnungsformat am 27. November 2019, also ein Jahr später, akzeptieren.

Neben dem XRechnungs-Format kann aber auch das bereits etablierte Datenaustauschformat ZUGFeRD verwendet werden. Vorausgesetzt, es entspricht wie

ZUGFeRD 2.0 allen Anforderungen der europäischen Norm. Die Vorläuferversion ZUGFeRD 1.0 hat bereits vor Jahren erfolgreich als elektronisches Rechnungsformat die Papierrechnung abgelöst. Diese Anwendung ist auch bereits seit Langem im gotomaxx PDFMAILER integriert. ZUGFeRD 1.0 vereint alle Vorteile der E-Rechnung, allerdings entspricht diese ZUGFeRD-Version nicht der EU-Norm.

Der neue PDFMAILER 6.1 enthält bereits ZUGFeRD 2.0. Der entscheidende Unterschied zu ZUGFeRD 1.0 liegt im Profil Comfort, denn das wird bei 2.0 zu Profil EN 16931 und ist nach Vorgaben der EU-Norm „fully com-

pliant“. Ein weiterer wichtiger Punkt der Version 2.0 ist die Möglichkeit, dass die zwei Repräsentanzen einer ZUGFeRD-Rechnung XML und PDF in getrennten Dateien – oder auch nur als rein strukturierte Daten in Form einer XML-Datei – versendet werden können. Denn die Hybridrechnung ist im europäischen Standard nicht mehr vorgesehen. PDFMAILER 6.1 kann außerdem Ihre Rechnung mit einem Klick in das XRechnungs-Format umwandeln. Das digitale Rechnungsformat basiert auf einem CEN-Standard (erarbeitet vom Europäischen Komitee für Normung) und verfolgt das Ziel, die europäische Norm in einen zwi-



schen Bund, Ländern und Kommunen abgestimmten nationalen Standard zu übertragen und darüber hinaus den Dokumentaustausch EU-weit zu vereinfachen. So sollen die Behörden zukünftig auch Rechnungen aus dem EU-Ausland problemlos empfangen können. Die XRechnung ist ein rein binäres und maschinenlesbares Format. Die gotomaxx Portalcloud ergänzt dieses binäre Format um ein Sichtformat, das auch für

den Menschen lesbar ist. Die Einführung der digitalen Rechnung bietet laut Innenministerium sowohl für die öffentliche Verwaltung als auch für deren Lieferanten Potenzial für Einsparungen, Effizienzsteigerungen und Verkürzungen der Durchlaufzeiten. Konkret bedeutet die Umstellung auf die Formate ZUGFeRD 2.0 oder XRechnung für öffentliche Auftraggeber eine Zeit- und Kostenersparnis durch automatisierte

Prozesse, einen kürzeren Rechnungsdurchlauf durch schnellere Freigabeprozesse und eine erhöhte Transparenz über den gesamten Bearbeitungsprozess. Der Rechnungssteller profitiert von Kosteneinsparungen durch die Nutzung der elektronischen Form, einer Liquiditätsverbesserung durch frühere Zahlungseingänge und weiteren Einsparungen durch die Optimierung interner Prozesse.

FAZIT

Die elektronische Rechnung nach EU-Norm in der öffentlichen Verwaltung kommt schon bald. XRechnung und ZUGFeRD 2.0 stehen als gleichberechtigte Rechnungsformate nebeneinander. Folgerichtig enthält PDFMAILER 6.1 auch die neue ZUGFeRD-Version 2.0 und eine Rechnung im Format XRechnung. So lässt sich die neue EU-Richtlinie unkompliziert, schnell und rechtskonform erfüllen.



© 2018