RÜESCH

Information zur EU-Datenschutzgrundverordnung (DSGVO)

Am 25. Mai 2018 tritt die EU-Datenschutzverordnung (DSGVO) der EU in Kraft. In diesem Dokument werden neben einer kurzen Einführung die in diesem Zusammenhang relevanten Aspekten in der die Firma Rüesch AG tätig ist beschrieben.

Version	1.00
Datum	30. April 2018
Autor	Ridvan Krasniqi

Rüesch AG
Rorschacherstrasse 70 | CH-9424 Rheineck | **Tel.** +41 71 886 47 47 | **Fax** +41 71 886 47 48 | info@ruesch-ag.ch | **www.ruesch-ag.ch**
CHE-101.132.662 MWST

RÜESCH

Information zur EU-Datenschutzgrundverordnung

Inhaltsverzeichnis

1 Einleitung 3

2 Einige wichtige Begriffe 4

2.1 Betroffener 4

2.2 Verantwortlicher 4

2.3 Personenbezogene Daten 4

2.4 Besondere Kategorien personenbezogener Daten 4

2.5 Verarbeitung 4

2.6 Einwilligung 5

2.7 Profiling 5

2.8 Empfänger 5

2.9 Auftragsverarbeiter 5

2.10 Datenschutzbeauftragter 5

2.11 Aufsichtsbehörde 5

3 Neuerungen 6

3.1 Information 6

3.2 Einwilligung 6

3.3 Privacy Breach 6

3.4 Recht auf Vergessenwerden und Portability 6

4 Wichtige Elemente der DSGVO 7

4.1 Personenbezogene Daten 7

4.2 Rechtmässigkeit der Verarbeitung 7

4.3 Rechte Betroffener 7

4.4 Informationspflicht 7

4.5 Pflicht zur Datenschutzfolgenabschätzung 8

4.6 Auftragsverarbeitung 8

5 Die wichtigsten Änderungen im Überblick 8

5.1 Cookies 8

5.2 Blog-Kommentare 8

5.3 Google Analytics 8

5.4 Newsletter 8

5.5 Social Media 9

5.6 Datenschutzerklärung und Impressum 9

5.7 SSL-Verschlüsselung 9

5.8 Werbung 9

5.9 Verzeichnis aller Tätigkeiten der Datenverarbeitung 9

Rüesch AG

Rorschacherstrasse 70 | CH-9424 Rheineck | **Tel.** +41 71 886 47 47 | **Fax** +41 71 886 47 48 | info@ruesch-ag.ch | **www.ruesch-ag.ch**

CHE-101.132.662 MWST

RÜESCH

Information zur EU-Datenschutzgrundverordnung

1 Einleitung

Ab dem 25. Mai 2018 wird die EU-Datenschutz-Grundverordnung (DSGVO) anwendbar sein. Diese ist nicht für alle Schweizer Unternehmen relevant – aber Schweizer Unternehmen, die Angebote in die EU bringen – z.B. ein Webshop betreiben, der sich auch an Konsumenten in Ländern in der EU wenden; nicht aber, wenn der Webshop nur Produkte oder Dienstleistungen in der Schweiz anbietet – oder wenn das Nutzerverhalten von EU-Bürgern und Bürgerinnen analysiert wird. Ebenfalls findet die DSGVO Anwendung im Rahmen von Outsourcing in die EU oder für ein EU-Unternehmen.

Damit ist aber auch klar, dass die DSGVO für viele, vor allem kleinere lokale Unternehmen keine Relevanz haben dürfte. Darum: Zuerst sorgfältig prüfen, ob die DSGVO anwendbar ist, bevor man in Aktivismus verfällt.

Ist die DSGVO anwendbar, gelten insbesondere folgende Punkte:

- Die Anforderungen an die Transparenz sind höher als bisher;
- Eine Einwilligung für eine Datenbearbeitung muss ausdrücklich erfolgen. Ein Hinweis in den AGB genügt definitiv nicht; zudem braucht es einen Hinweis auf die jederzeitige Widerrufsmöglichkeit;
- Datenportabilität muss gewährleistet sein, das heisst, ein Nutzer muss seine Daten zu einem anderen Dienstleistungsanbieter mitnehmen können in strukturierter und maschinenlesbarer Form;
- Besteht ein hohes Risiko für die Rechte und Freiheiten der betroffenen Person, muss der Verantwortliche der Datenbearbeitung eine sogenannte Datenschutzfolgeabschätzung durchführen. Das bedeutet, es müssen die Risiken identifiziert und allfällige Gegenmassnahmen vorbereitet sein;
- Bei automatisierten Entscheiden besteht ein Anrecht auf Beurteilung durch einen Menschen
- Voreinstellungen sollten «Privacy»-freundlich sein

Einen betrieblichen Datenschutzbeauftragten braucht es nur, wenn eine Kerntätigkeit des Unternehmens in der Bearbeitung besonders schützenswerter Personendaten besteht oder eine umfangreiche, systematische Personenüberwachung erfordert.

Wie die neusten Ereignisse zeigen, muss unbedingt der Datensicherheit genügend Aufmerksamkeit geschenkt werden. Denn je mehr Daten elektronisch bearbeitet werden, desto attraktiver wird ein Hacking.

Dieses Dokument enthält einige wichtige Informationen für die Umsetzung der Datenschutzgrundverordnung in ihrem Unternehmen. Bitte beachten Sie, dass neben der Datenschutzgrundverordnung der EU auch noch weitere länderspezifische Gesetze zu beachten sind. Trotz sorgfältigster Bearbeitung erfolgen sämtliche Angaben ohne Gewähr, eine Haftung der Rüesch AG ist ausgeschlossen.

Für weiter Informationen wenden Sie sich bitte an Ihren Rechtsberater.

Rüesch AG
Rorschacherstrasse 70 | CH-9424 Rheineck | **Tel.** +41 71 886 47 47 | **Fax** +41 71 886 47 48 | info@ruesch-ag.ch | **www.ruesch-ag.ch**
CHE-101.132.662 MWST

2 Einige wichtige Begriffe

2.1 Betroffener

Darunter versteht man die betroffene (natürliche) Person, deren Daten geschützt werden sollen.

2.2 Verantwortlicher

Die natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet.

2.3 Personenbezogene Daten

Alle Informationen, die sich auf eine Identifizierte oder identifizierbare natürliche Person beziehen; als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind, identifiziert werden kann.

Wenn sich Daten z.B. einer IP-Adresse zugeordnet werden können, gelten diese ebenfalls als personenbezogen.

2.4 Besondere Kategorien personenbezogener Daten

Für sensible personenbezogene Daten gelten höhere Anforderungen und betreffen

- Politische Überzeugungen
- Genetische Daten
- Biometrische Daten
- Rasse oder ethnische Zugehörigkeit
- Religions- oder Glaubenszugehörigkeit
- Gesundheitsdaten / Sexuelle Orientierung
- Gewerkschaftszugehörigkeit
- Strafurteile

2.5 Verarbeitung

Jeden mit oder ohne Hilfe automatisierter Verfahren ausgeführten Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten wie das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung

2.6 Einwilligung

Jede freiwillig für den bestimmten Fall, in informierter Weise und unmissverständlich abgegebene Willensbekundung in Form einer Erklärung oder einer sonstigen eindeutigen bestätigenden Handlung, mit der die betroffene Person zu verstehen gibt, dass sie mit der Verarbeitung der sie betreffenden personenbezogenen Daten einverstanden ist.

In den meisten Fällen ist eine Verarbeitung von personenbezogenen Daten nur dann zulässig, wenn die betroffene Person dazu die Einwilligung gibt.

2.7 Profiling

Jede Art der automatisierten Verarbeitung personenbezogener Daten, die darin besteht, dass diese personenbezogenen Daten verwendet werden, um bestimmte persönliche Aspekte, die sich auf eine natürliche Person beziehen, zu bewerten, insbesondere um Aspekte bezüglich Arbeitsleistung, wirtschaftliche Lage, Gesundheit, persönliche Vorlieben, Interessen, Zuverlässigkeit, Verhalten, Aufenthaltsort oder Ortwechsel dieser natürlichen Person zu analysieren oder vorherzusagen.

2.8 Empfänger

Natürliche oder juristische Person, der personenbezogene Daten offengelegt werden.

2.9 Auftragsverarbeiter

Eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet.

2.10 Datenschutzbeauftragter

Die Digitalisierung durchdringt zunehmend auch den Staat und die öffentliche Verwaltung. Mit dem Einsatz der neuen Technologien findet ein gesellschaftlicher Wandel statt.

Aus der Sicht des Datenschutzbeauftragten muss eine Strategie der öffentlichen Verwaltung zur Digitalisierung festhalten, dass die Digitalisierung zur Stärkung des Rechtsstaats und der föderalen Demokratie beitragen soll.

- hat gesetzlich definierte Aufgaben und Verantwortlichkeiten
- kann ein interner Mitarbeiter sein (kann aber auch eine externe Person sein)

Die Datenschutz-Grundverordnung schreibt unter gewissen Umständen die Installation eines Datenschutzbeauftragten vor, für Rüesch AG ist dies aber nicht erforderlich.

2.11 Aufsichtsbehörde

Jeder Mitgliedstaat sieht vor, dass eine oder mehrere unabhängige Behörden für die Überwachung der Anwendung dieser Verordnung zuständig sind, damit die Grundrechte und Grundfreiheiten natürlicher Personen bei der Verarbeitung geschützt werden und der freie Verkehr personenbezogener Daten in der Union erleichtert wird (im Folgenden „Aufsichtsbehörde“).

3 Neuerungen

Im Vergleich zum heutigen Schweizer Recht bringt die DSGVO verschiedene wichtige Neuerungen.

3.1 Information

Neu sind die betroffenen Personen grundsätzlich über die Datenbearbeitung zu informieren. Die Information muss "in präziser, transparenter, verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache" erfolgen. Der Umfang der Information wird vorgegeben, ist beträchtlich und umfasst u.a. den Zweck und die Rechtsgrundlage der Bearbeitung, berechtigte Interessen, auf welche sich der Verarbeiter stützt, die Empfänger der Daten, die angemessenen Garantien, auf welche sich ein internationaler Datentransfer stützt (inkl. dem Verweis auf die Möglichkeit, eine Kopie davon zu erhalten), die Dauer der Speicherung sowie eine ausdrückliche Information über die Rechte der betroffenen Personen.

3.2 Einwilligung

Dieselben Anforderungen geltend für die Form der Einwilligung, wenn die Bearbeitung auf einer Einwilligung beruht. Die Einwilligung hat "in verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache" zu erfolgen. Besondere Vorsicht ist geboten, wenn eine Dienstleistung von der Einwilligung zur Verarbeitung von Personendaten abhängig gemacht wird, welche für die Erbringung der Dienstleistung nicht erforderlich sind. Die Einwilligung ist zudem jederzeit widerrufbar. Jugendliche ab dem Alter von 16 Jahren dürfen die Einwilligung bei Online-Angeboten selbst erteilten, doch können Mitgliedsstaaten das Mindestalter bis auf 13 Jahre reduzieren. Bei Kindern unter dem Mindestalter ist die Zustimmung der Eltern erforderlich, was soweit möglich auch technisch sicherzustellen ist.

3.3 Privacy Breach

Bei Sicherheitslücken muss inskünftig die zuständige Aufsichtsbehörde unverzüglich und möglichst binnen 72 Stunden nach der Entdeckung der Sicherheitslücke benachrichtigt werden. Nur wenn kein Risiko für die Rechte und Freiheiten der betroffenen Personen besteht, kann darauf verzichtet werden. Durch technische und organisatorische Massnahmen ist sicherzustellen, dass Sicherheitslücken sofort entdeckt werden. Die betroffenen Personen selbst sind zu benachrichtigen, wenn voraussichtlich ein hohes Risiko für deren Rechte und Freiheiten besteht. Die Benachrichtigung hat unverzüglich und in einfacher und klarer Sprache zu erfolgen.

3.4 Recht auf Vergessenwerden und Portability

Den betroffenen Personen steht – ähnlich wie im Schweizer Recht – grundsätzlich das Recht zu, die Löschung ihrer Daten zu verlangen. Die Löschung hat unverzüglich zu erfolgen. Zudem haben die betroffenen Personen neu das Recht, Daten, die sie dem Verarbeiter selbst zur Verfügung gestellt haben, in einem gängigen maschinenlesbaren Format herauszuverlangen oder auf einen Nachfolger übertragen zu lassen (sog. data portability). Ob dieses auf Facebook und ähnliche soziale Netzwerke gemünzte 'Recht auf Datenübertragbarkeit' auch auf andere Fälle wie z.B. Banken, Versicherungen, Buchungsportale, Online-Shops oder ähnliches Anwendung findet, muss sich weisen. Die fristgerechte Erfüllung dieser Rechte bedarf in vielen Fällen technischer Anpassungen.

Rüesch AG
Rorschacherstrasse 70 | CH-9424 Rheineck | **Tel.** +41 71 886 47 47 | **Fax** +41 71 886 47 48 | info@ruesch-ag.ch | **www.ruesch-ag.ch**
CHE-101.132.662 MWST

4 Wichtige Elemente der DSGVO

4.1 Personenbezogene Daten

Alle Daten, die sich auf eine bestimmte oder bestimmbare natürliche Person beziehen.

Die DSGVO regelt nur den Umgang mit Daten natürlicher Personen, die Daten juristischer Personen werden von der DSGVO nicht behandelt.

Mit hoher Wahrscheinlichkeit verwalten wir mit unseren Systemen keine sensiblen personenbezogenen Daten.

4.2 Rechtmässigkeit der Verarbeitung

Eine Verarbeitung ist nur rechtmässig, wenn sie auf einer Rechtsgrundlage basiert.

Rechtsgrundlagen können sein:

- Sie sind gesetzlich dazu verpflichtet, personenbezogene Daten zu verarbeiten
- Die Verarbeitung personenbezogener Daten ist für die Abwicklung eines Vertrages erforderlich.
- Die Verarbeitung personenbezogener Daten ist für vorvertragliche Massnahmen erforderlich
- Der Betroffene hat der Verarbeitung zugestimmt (mit der Einwilligung)

4.3 Rechte Betroffener

Die betroffenen Personen erhalten erweiterte Rechte ("betroffenenrechte")

Recht auf...

- Auskunft
- Berichtigung
- Löschung
- Einschränkung der Verarbeitung / Widerspruchsrecht
- Datenübertragbarkeit
- Beschwerdemöglichkeit

4.4 Informationspflicht

Sie sind verpflichtet, die Betroffenen über die Verarbeitung personenbezogener Daten zu informieren:

- Kontaktdaten des für die Verarbeitung Verantwortlichen
- Kontaktdaten eines allfälligen Datenschutzbeauftragten
- Empfänger oder Kategorien von Empfängern der Daten
- Information, falls Daten an Drittstaaten transferiert werden
- Angabe zur Speicherdauer personenbezogener Daten
- Information über das Bestehen der Betroffenenrechte

4.5 Pflicht zur Datenschutzfolgenabschätzung

Datenschutzfolgeabschätzungen sind notwendig, wenn neue Technologien erhebliche Risiken für die Rechte und Freiheiten natürlicher Personen zur Folge haben könnten.

Wir gehen davon aus, dass dies für Sie in Zusammenhang mit der Rüesch AG eher nicht relevant sein wird.

4.6 Auftragsverarbeitung

Wenn Sie personenbezogene Daten an Dritte zwecks weiterer Verarbeitung übergeben sind Sie verpflichtet, mit dem Dienstleister einen sogenannten "Auftragsverarbeitungsvertrag" abzuschliessen.

Rüesch AG tritt mit Ihnen voraussichtlich in folgenden Fällen als Auftragsverarbeiter auf:

- Zugriff auf Ihr System via Fernwartung im Rahmen der Hotline
- Zugriff auf Ihr Hosting via Anmeldedaten im Rahmen des Supports / Wartung

5 Die wichtigsten Änderungen im Überblick

5.1 Cookies

Mit am stärksten im Fokus stehen ab 25. Mai 2018 sicher die Cookies. Die kleinen Dateien auf den Rechnern der Nutzer sorgen seit vielen Jahren für Diskussionen. Durch die DSGVO wurde die Definition personenbezogener Daten nochmal verschärft und es ist davon auszugehen, dass Cookies nun noch kritischer gesehen werden. Deshalb werden aktuell immer öfters mehr Webseiten auf die Cookies aufmerksam gemacht.

5.2 Blog-Kommentare

Ein oft unterschätztes Problem sind Kommentare in Blogs. Hier werden in der Regel Mail- und IP-Adressen der Nutzer gespeichert, die einen Kommentar hinterlassen. Das sind natürlich personenbezogene Daten.

5.3 Google Analytics

Viele Website-Betreiber nutzen Tracking-Services wie Google Analytics. Auch hier muss man natürlich im Hinblick auf die DSGVO genauer hinschauen.

Google Analytics hat allerdings schon in der Vergangenheit Vorkehrungen getroffen, Datenschutzanforderungen zu erfüllen. Wenn man dann noch dafür sorgt, dass die IPs anonymisiert übertragen werden, sollte das auch in Zukunft kein Problem darstellen.

5.4 Newsletter

Für die Newsletter gelten auch die DSGVO. So haben Services wie "CleverReach" oder "MailChimp" ausgereifte Systeme für die Nutzer und deren An- und Abmeldungen automatisch und problemlos zu ermöglichen und zudem die Handlungen der Nutzer zu dokumentieren.

5.5 Social Media

Schon aktuell wird dringend davon abgeraten, die offiziellen Plugins/Buttons der sozialen Netzwerke auf der eigenen Website zu nutzen. Diese übermitteln sogar schon beim Betreten der Website Daten an den jeweiligen Anbieter, egal ob man dort Mitglied ist oder nicht.

Deshalb wird die DSGVO hier noch strenger sein, so dass sich an dieser Empfehlung auch nichts ändert.

5.6 Datenschutzerklärung und Impressum

Jede Website sollte eine Datenschutzerklärung enthalten. Diese ist aber das kleinste Problem. Es gibt bereits heute Online-Generatoren, mit deren Hilfe man eine passende Datenschutzerklärung für die eigene Website erstellen kann. Das wird in Zukunft sicher auch so bleiben. Man sollte nur daran denken, Anfang kommenden Jahres die eigene Datenschutzerklärung zu aktualisieren.

Natürlich ist es dann auch notwendig das Impressum anzupassen.

5.7 SSL-Verschlüsselung

Mal abgesehen davon, dass Google gern nur noch SSL-verschlüsselte Websites möchte und auch die Browser unverschlüsselte Websites schon (negativ) hervorheben, wird mit der DSGVO die Verschlüsselung wohl endgültig Pflicht.

Der Datenschutz "by Design" bzw. "by Default" legt einfach nahe, dass jegliche Datentransfers über das Netz nur noch verschlüsselt erfolgen sollten. Wir haben an allen unseren Websites und Kundenwebsites mit der Umstellung auf SSL begonnen und werden das auch in der Zukunft so handhaben.

5.8 Werbung

Die neuen Datenschutzrichtlinien werden auch die Werbung im Netz beeinflussen. Ein normales Baner ohne Tracking ist zwar kein Problem, aber Methoden wie Frequency Capping oder Re-Marketing werden in der heutigen Form nicht mehr möglich sein.

5.9 Verzeichnis aller Tätigkeiten der Datenverarbeitung

Es wird gefordert, dass man die Verarbeitung personenbezogener Daten in einem Verzeichnis klar und transparent beschreibt. Also auch, was mit den Daten passiert.

Das sind sicher nicht alle Website-Aspekte, auf die die DSGVO in Zukunft Einfluss haben wird, aber es sind die wichtigsten und es sollten erste Anpassungen stattfinden.

Rüesch AG
Rorschacherstrasse 70 | CH-9424 Rheineck | **Tel.** +41 71 886 47 47 | **Fax** +41 71 886 47 48 | info@ruesch-ag.ch | **www.ruesch-ag.ch**
CHE-101.132.662 MWST