So bereiten Sie sich auf die DSGVO vor

Eine neue Gesetzgebung der Europäischen Union tritt demnächst in Kraft, die das Thema Sicherheit und Datenschutz genauer unter die Lupe nimmt. Die Datenschutz-Grundverordnung, kurz DSGVO, **regelt den Umgang von Organisationen mit Daten europäischer Bürger,** bei denen sehr spezifische Richtlinien vorliegen und bei einem Verordnungsverstoß hohe Strafen folgen.

Unser Whitepaper wird Ihnen die neue Verordnung erklären und zeigen, wie Sie sich darauf vorbereiten können. Wir werden Ihnen einige Werkzeuge vorstellen, mit denen Sie überprüfen können, ob Ihre Organisation den Richtlinien der DSGVO entspricht und Ihnen die notwendigen Schritte zeigen diese einzuhalten.

FFW

Kontaktieren Sie uns

Damit Sie alle Vorkehrungen für die neue DSGVO treffen können, sollten Sie sich im Klaren sein welche Daten Sie erheben, wo und wie Sie diese verarbeiten und speichern sowie auf welche Weise Ihre Organistion die Userrechte innerhalb Ihrer Systeme schützen kann.

Wir unterstützen Sie gerne bei den Vorbereitungen für die neue DSGVO.

Erfahren Sie mehr auf:

ffwagency.com facebook twitter linked in

Was ist die DSGVO?

Die EU hat 2016 die Datenschutz-Grundverordnung (DSGVO) veranlasst, um Daten von EU-Bürgern zu schützen: **„Diese Verordnung enthält Vorschriften zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Verkehr solcher Daten."**

Doch was genau heißt das?

In der EU gibt es zwei Gesetzestypen:

Richtlinien,
bei denen das Parlament das Gesetz verabschieden muss

Verordnungen,
die sofort in den Mitgliedsstaaten gelten müssen

Die DSGVO ist eine Verordnung, die ab dem 25. Mai. 2018 in allen Mitgliedsstaaten der EU gleichermaßen gilt. Sie gilt auch für Organisationen, deren Sitz außerhalb der EU liegt, die aber Daten von EU-Bürgern sammelt, speichert oder sich zu Nutze macht.

Was beim Lesen der DSGVO auffällt, ist folgende wiederkehrende Formulierung: **„Recht über den Schutz natürlicher Personen in Bezug auf die Verarbeitung personenbezogener Daten".**

Diese Formulierung ist besonders wichtig zu beachten, da sie verschiedene rechtliche Bedeutungen hat:

Eine **natürliche Person** ist jeder lebende Mensch

Persönliche Daten sind sämtliche Daten, die auf eine natürliche Person zustimmen. Das könnten Namen, Identifikationsnummern, Ortungsdaten, Online-Daten oder andere beliebige Daten sein im Bezug auf die physische, physiologische, geschlechtliche, mentale, wirtschaftliche, kulturelle oder soziale Identität einer natürlichen Person.

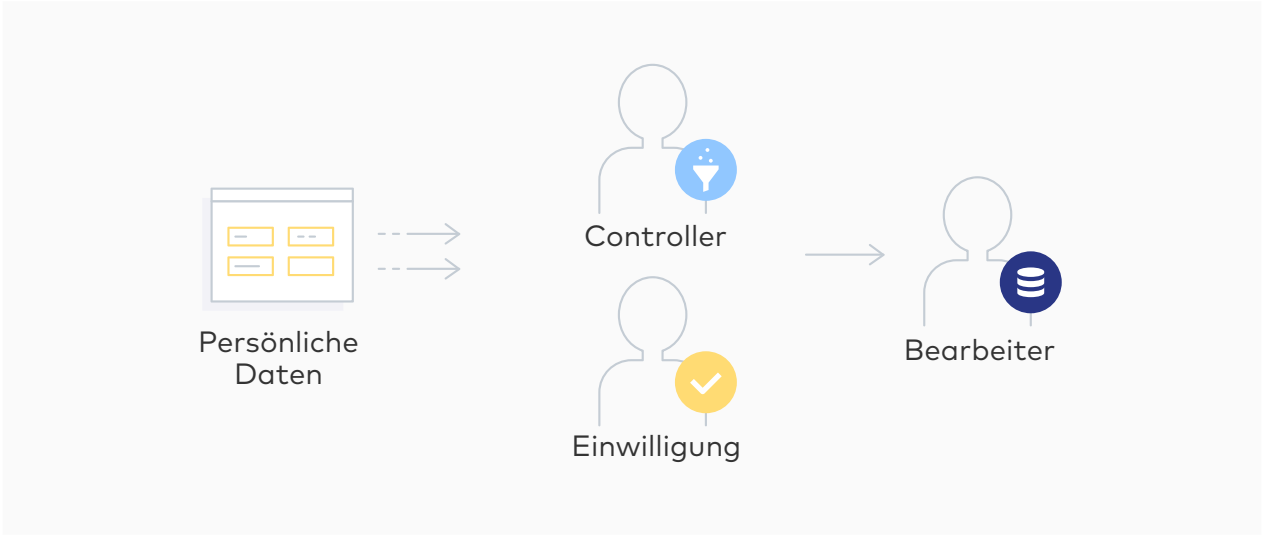
Verarbeitung bedeutet die Nutzung oder Verwendung solcher persönlichen Daten. Das betrifft beispielsweise das:

- Sammeln
- Aufnehmen
- Sortieren
- Speichern
- Anpassen
- Abrufen
- Nutzen
- Übertragen
- Verbreiten
- Löschen oder Zerstören solcher Daten

Organisationen, die persönliche Daten verlieren, beispielsweise Talk Talk, die Daten von 170.000 Personen verloren haben, dürfen mit hohen Strafen rechnen. **Im Idealfall sind nur 10 Millionen Euro beziehungsweise 2% Jahresumsatzes fällig** (je nachdem, welcher Betrag größer ist). Bei Härtefällen verdoppeln sich diese Zahlen.

Für wen gilt die DSGVO?

Ganz einfach: für alle. Wenn es auch nur den Hauch der Chance gibt, dass sich im System Ihrer Organisation irgendwo Daten eines EU-Bürgers befinden, müssen Sie sicherstellen, dass Sie nicht gegen dieses neue Gesetz verstoßen.



Controller

Ein Controller ist die Organisation oder eine Einzelperson, der für die Daten zuständig ist. Offiziell betrachtet, bestimmt ein Controller den Zweck und die Verarbeitungsschritte persönlicher Daten.

Ein Controller kann eine natürliche oder juristische Person, Behörde, Agentur oder eine andere Körperschaft sein, die entweder alleine oder zusammen mit anderen agiert.

Wenn Sie beispielsweise dieses Whitepaper von FFW herunterladen, haben Sie Ihren Namen, Ihre E-Mail-Adresse und womöglich einige Informationen über Ihren Arbeitgeber angegeben. Dies macht uns zum Controller dieser Daten.

Einwilligung

Der Controller ist für die legale, gerechte und transparente Verarbeitung der Daten verantwortlich. Controller dürfen Daten im Rahmen des Gesetzes verarbeiten, sofern die Dateninhaber zur Verarbeitung ihrer persönlichen Daten zugestimmt haben. Die Einwilligung muss aus freien Stücken geschehen und die Wünsche des Dateninhabers auf unmissverständliche Weise wiedergeben.

Das Gesetz stellt klar und deutlich fest, was Einwilligung bedeutet: erst bei einer eindeutigen Einwilligung, dürfen die Daten des zugestimmten Users genutzt werden.

Es besteht die Pflicht dem User einen klar verständlichen Datenschutzhinweis zu geben, sobald seine Daten eingegeben wurden. Dieser Hinweis muss eindeutig erklären, warum um die Einwilligung gebeten wird und was genau mit den Daten geschehen wird. Außerdem müssen User immer aktiv die Bearbeitung bzw. die Nutzung der Daten erlauben, statt die Bearbeitung und Nutzung der Daten zu untersagen. Manipulative Formulierungen und bereits ausgefüllte oder angekreuzte Formularfelder gelten als Gesetzesverstoß. Als Controller müssen Sie sich im Klaren sein, dass Sie um die Genehmigung der Nutzung Ihrer Userdaten bitten und was es bedeutet, wenn Sie nach dieser Genehmigung bitten.

Bearbeiter

Der Bearbeiter ist eine Person oder Organisation, die die Daten bearbeitet, speichert oder zerstört. Wie auch der Controller kann der Bearbeiter eine natürliche oder juristische Person, Behörde, Agentur oder eine andere Körperschaft sein.

Ein Bearbeiter kann die Daten im Auftrag eines Controllers verarbeiten.

Wir bspw. sind Datenverarbeiter, da wir über einige unserer Services Userdaten empfangen und diese dadurch bei uns gespeichert sind. Das macht uns zum Bearbeiter für Daten Dritter, auch wenn wir diese Daten aus unternehmerischen Gründen nicht anrühren.

Bei der DSGVO dreht es sich um Privatsphäre und Datenschutz

Die DSGVO macht sehr deutlich, dass Organisationen in der Lage und bereit sein müssen, die Einhaltung dieses Gesetzes aufzuzeigen. Das Ziel für Organisationen sollte also sein, proaktiv an die Sache heranzugehen und nicht erst dann zu reagieren, wenn es zu spät ist. Sobald Sie von jemandem kontaktiert und gefragt werden, ob Sie den Richtlinien der DSGVO entsprechen, sollten Sie zweifelsfrei und sofort aufzeigen können, dass Ihre Organisation die 6 Richtlinien der DSGVO umgesetzt hat.

Laut DSGVO müssen alle Daten...

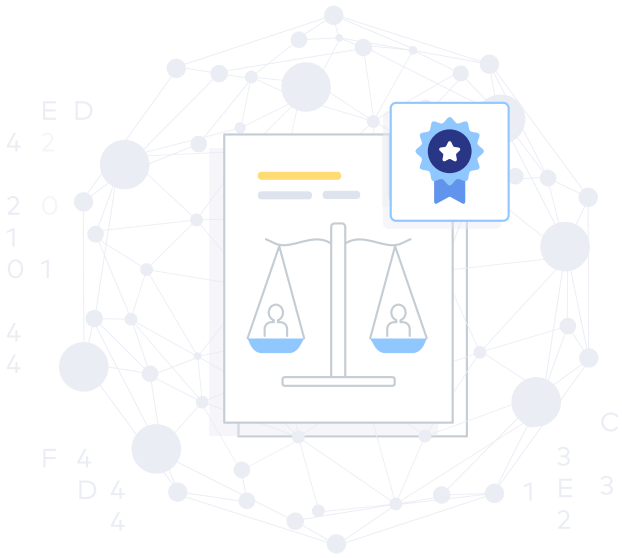
1. rechtmäßig, gerecht und in transparenter Weise verarbeitet werden
2. für bestimmte, explizit genannte und legale Zwecke gesammelt werden
3. stets auf dem neuesten Stand gehalten werden
4. auf das Nötigste beschränkt werden
5. nur so lange zur Identifizierung von Personen eingesetzt werden als unbedingt notwendig
6. so verarbeitet werden, dass deren Sicherheit gewährleistet wird

In anderen Worten heißt dies nichts Anderes als Folgendes:

Daten dürfen nur mit der ausdrücklichen Einwilligung gesammelt werden, wobei alle User genau wissen sollten, wofür Ihre Daten verwendet werden. Das Sammeln und Aufbewahren von Daten sollte nur auf das Notwendigste pro User beschränkt werden. Ihre Organisation sollte aufzeigen können, dass eine Anfrage zur Einwilligung unmissverständlich versendet wurde und dass die Daten nicht verkauft, modifiziert oder anderweitig missbraucht werden. Systeme für Marketingzwecke sollten nicht auf veralteten Daten basieren. Falls User ihre Daten aktualisieren oder ihre Einwilligung zurückziehen möchten, sollte dies so einfach wie möglich gemacht werden.

Vor allem aber, müssen die Daten an einem sicheren Ort gespeichert und verarbeitet werden, um die Privatsphäre der Dateninhaber zu schützen.

Userrechte leicht erklärt



Die DSGVO-Richtlinien wurden für EU-Bürger und zum Schutz ihrer persönlichen Daten konzipiert.
Diese Rechte beinhalten:

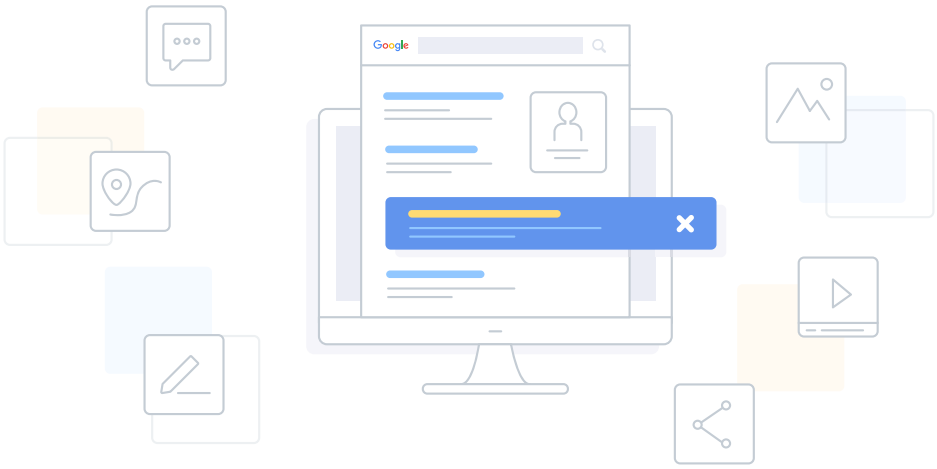
- das Recht, Informationen zu erhalten
- das Zugangsrecht
- das Korrekturrecht
- das Löschrecht
- das Recht, Bearbeitungen einzuschränken
- das Recht zur Datenübertragung
- das Widerspruchsrecht
- das Recht, nicht Teil automatisierter Entscheidungsprozesse sowie von Profiling zu werden

Sie müssen sichergehen, dass Sie und Ihre Organisation diese Richtlinien beim Sammeln, Speichern und sicheren Verarbeiten von Daten einhalten und zudem auch noch gewährleisten können, dass Sie über Systeme verfügen, mit denen EU-Bürger ihre Datenrechte in Anspruch nehmen können. **Dazu sollten Sie Prozesse, Verfahren und Schulungen für Ihr Personal einführen, um diese Richtlinien einzuhalten.**

Sämtliche Kommunikationskanäle müssen präzise und leicht verständlich sein. Seien Sie deshalb klar und deutlich mit Ihren Formulierungen – besonders bei rechtlichen Inhalten - sodass diese von der breiten Masse gut verstanden werden.

Ein Beispiel für den Aufbau eines Datenrecht-Frameworks

Wie können Sie nun sichergehen, dass Ihr System all diesen Richtlinien entspricht? Nehmen wir Google als Beispiel: Im Mai 2015 hat der Europäische Gerichtshof (EuGH) festgelegt, dass Suchmaschinen für die verlinkten Inhalte verantwortlich sind und dass Suchmaschinen folglich sichergehen müssen, dass diese mit den EU-Datenschutzrechten einhergehen. Ins Besondere wurde Google belehrt, dass sie das Recht auf Vergessenwerden einhalten müssen.



Laut Reuters „können Internet-Unternehmen dazu gezwungen werden, irrelevante oder zu persönliche Informationen aus Suchergebnissen zu entfernen. Der Europäische Gerichtshof (EuGH) hat die Klage eines Spaniers stattgegeben, in der er sich beschwerte, dass in Suchmaschinen ein Zeitungsartikel von 1998 zur Zwangsversteigerung seines Hauses unter seinem Namen erschien". Diesem Präzedenzfall zufolge sollten „nicht-öffentliche Personen in der Lage sein, ihre digitalen Spuren im Internet zu entfernen".

Um dem Recht auf Vergessenwerden gerecht zu werden, hat Google ein Framework entwickelt, um Suchergebnisse aus dem EU-Index zu entfernen. Gleichermaßen wurde ein Prozess für User eingerichtet, um die Entfernung von persönlichen Informationen zu verlangen. Dies ist ein klares Beispiel dafür, wie ein riesiger Konzern Prozesse und Prozeduren für User einrichtet, damit deren Rechte gewahrt werden. Das heißt, Ihre Organisation sollte ebenso in der Lage sein diesen Prozess in Ihren Systemen einzuführen, um nicht gegen die DSGVO zu verstoßen.

Die Implementierung eines DSGVO-Plans in 8 Schritten

Der erste Schritt zur Vorbereitung auf die DSGVO lautet, Ihre bestehenden Richtlinien und Prozesse in Ihrer Organisation zu bewerten. Welche Daten sammeln Sie und warum? Sind diese Daten sicher? Können User ihre Daten in Ihren Systemen entfernen? Richten Sie Prozesse, Verfahren und Trainingseinheiten für Ihr Personal ein, damit Ihre Organisation in der Lage ist den Ansprüchen und Rechten Ihrer User gerecht zu werden.

Davon abgesehen gibt es einige grundlegende Aspekte, die Sie zur Vorbereitung beachten sollten:

1. Aufklärung

Stellen Sie sicher, dass die Entscheidungsträger und Schlüsselpersonen Ihrer Organisation von der neuen DSGVO wissen und nötige Änderungen treffen. Geben Sie ihnen so bald wie möglich Bescheid, da Sie eventuell deren Zusage brauchen, um Änderungen in Ihren Systemen überhaupt in Angriff nehmen zu können.

2. Führen Sie ein Informationstechnik-Audit durch

Dokumentieren Sie, über welche persönlichen Daten Sie verfügen, woher Sie diese erhalten haben und mit wem Sie diese teilen.
Als Teil des Audits müssen Sie auch Ihre aktuellen Datenschutzrichtlinien überprüfen und einen Plan erstellen, um nötige Änderungen durchzuführen. Überprüfen Sie auch, welche Verfahren vorhanden sind, damit EU-Bürger ihre Rechte auf Ihrer Website wahrnehmen können. Usern sollte es möglichst leichtgemacht werden, ihre persönlichen Daten in den Systemen Ihrer Organisation einzugeben, zu aktualisieren oder auch zu löschen.

3. Richten Sie einen Plan ein, um Zugangsanfragen bearbeiten zu können

Wenn Sie von einer Einzelperson oder einer Behörde darum gebeten werden, die Einhaltung dieses Gesetzes nachzuweisen, werden Sie immer über einen Plan verfügen müssen. Stellen Sie sicher, dass Sie vorhandene Verfahren zur Datenlieferung aktualisieren (oder falls nicht vorhanden, diese zu erstellen), damit Sie solche Anfragen bearbeiten können.

4. Identifizieren Sie die rechtmäßige Verarbeitungsgrundlage

Seien Sie sich im Klaren, wie Sie Daten verarbeiten, aus welchen Gründen Sie diese verarbeiten und stellen Sie sicher, dass Ihre User für diese Verarbeitungen ihre explizite Einwilligung gegeben haben. Sie müssen sichergehen, dass Sie Userdaten rechtmäßig verarbeiten, die nötigen Dokumentationen darüber verfügen und dass die Datenschutzrichtlinien aktualisiert wurden, noch bevor die DSGVO geltendes Gesetz wird.

5. Überprüfen Sie Ihr System im Bezug auf Minderjährige

Dies ist ein äußerst wichtiger Schritt und leider ein Aspekt, den viele Organisationen zu übersehen scheinen. Je nachdem, welche Daten Sie sammeln, benötigen Sie möglicherweise Systeme, um das Alter Ihrer User zu überprüfen und die Einwilligung der Eltern oder Aufsichtspersonen zu erhalten.

6. Entwickeln Sie einen Plan für Datenverluste

Keine Organisation möchte ihre Daten verlieren. Stellen Sie also zunächst sicher, dass Ihre Userdaten bestmöglich gesichert sind. Weiterhin müssen Sie zusehen, entsprechende Verfahren und Systeme zu verwenden, um Verluste persönlicher Daten zu erkennen, zu melden und zu untersuchen. Um zu gewährleisten, dass Ihre Systeme den neuen Richtlinien entsprechen, sollten Sie sich mit den Hinweisen im Artikel 29 der Arbeitsgruppe befassen. Außerdem sollten Sie ausarbeiten, wie Sie in Ihrer Organisation eine Datenschutz-Verträglichkeitsprüfung implementieren können.

7. Datenschutzbeauftragte

Beauftragen Sie jemanden innerhalb Ihrer Organisation oder eine juristische Person, die die Verantwortung für den Datenschutz übernimmt und stellen Sie fest, wo sich diese Rolle innerhalb Ihrer Organisationsstruktur befindet und halten Sie Ihren Datenbeauftragten namentlich fest.

8. Verstehen Sie internationale Richtlinien

Falls Ihre Organisation in mehr als nur einem Mitgliedsstaat operiert, bestimmen Sie bitte Ihre zutreffende Datenschutzaufsichtsbehörde. Sie wissen nicht, wo Sie überhaupt anfangen sollen? Im Dezember 2016 hat die Arbeitsgruppe des Artikels 29 ihre Hinweise zum Identifizieren der Haupt-Aufsichtsbehörde veröffentlicht, um Organisationen bei diesem Schritt zu helfen. Um die Identifikation der über allem stehenden Aufsichtsbehörde weiter zu vereinfachen, müssen Sie verstehen, an welchen Stellen Ihre Organisation im Bezug auf Datenverarbeitungen Entscheidungen trifft.

Ernennen Sie einen Vertreter

Organisationen, die ihren Hauptsitz außerhalb der EU haben, jedoch innerhalb der EU operieren oder persönliche Daten von EU-Bürgern verarbeiten, müssen einen Repräsentanten innerhalb der EU finden.

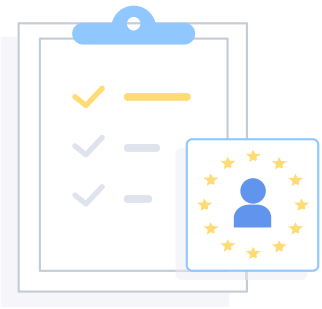
Laut Artikel 4 der DSGVO,
„können alle natürlichen oder juristischen Personen, die in einem Mitgliedsstaat der EU ansässig sind, als Repräsentant in der EU für Unternehmen agieren, welche ihren Sitz nicht in der EU haben".

Es liegt in der Verantwortung des Repräsentanten die, von Aufsichtsbehörden angefragten, Informationen bereitzustellen.

Sobald ein Repräsentant gefunden wurde, müssen Sie diese Person schriftlich als den Repräsentanten Ihrer Organisation bestimmen. Ein Repräsentant vertritt den Controller oder den Berarbeiter hinsichtlich ihrer Verpflichtungen der DSGVO.

Einige Hinweise zu den Repräsentanten:

- Ein Repräsentant muss in einem der EU-Mitgliedsstaaten ansässig sein, in dem Sie auch persönliche Daten sammeln.
- Es liegt in Ihrer Verantwortung, einen Repräsentanten zu ernennen, der vorurteilslos rechtliche Schritte verfolgt, die sich auch gegen Ihr Unternehmen richten könnten.
- Der Repräsentant unterliegt möglichen rechtlichen Schritten im Fall eines Verstoßes des Unternehmens gegen die DSGVO. Dies bedeutet, dass sowohl Ihr Unternehmen als auch Ihr Repräsentant mit Strafen rechnen müssen, sofern Sie sich nicht an das Gesetz halten.



Die DSGVO rückt immer näher und viele der Dienstleister, von den Organisationen der EU, müssen noch Repräsentanten ernennen.

Die nächsten Schritte

Damit Sie alle Vorkehrungen für die neue DSGVO treffen können, sollten Sie sich im Klaren sein welche Daten Sie erheben, wo und wie Sie diese verarbeiten und speichern sowie auf welche Weise Ihre Organistion die Userrechte innerhalb Ihrer Systeme schützen kann.

Wir empfehlen Ihnen, zunächst zu identifizieren, wie persönliche Daten auf Ihrer Website verwendet werden.

Sobald Sie erkannt haben, welche Daten Sie wie genau nutzen, können Sie damit beginnen Systeme zu erstellen, welche die Privatsphäre Ihrer User besser schützen und Verfahren einzurichten, damit User Ihrer Systeme ihre persönlichen Daten aufrufen, aktualisieren oder löschen können.

Wir unterstützen Sie gerne bei den Vorbereitungen für die neue Verordnung. Unser DSGVO Paket analysiert nicht nur Ihre digitale Präsenz, um mögliche Verstöße zu identifizieren, sondern liefert auch Empfehlungen und Verbesserungsvorschläge und minimiert die Gefahr von Strafen bei Gesetzesverstößen.

Kontaktieren Sie uns und einer unserer DSGVO Experten wird sich direkt bei Ihnen melden, um Ihnen behilflich sein.