WHITE PAPER

Agiloft

GDPR: What You Need to Know

Introduction

On May 25, 2018, the European Union's General Data Protection Regulation (GDPR) goes into effect. This is a major change in privacy law that will affect every organization that collects or processes data in the European Union (EU). The GDPR codifies the data privacy rights of not just EU citizens but also of anyone whose personal data is collected or processed in the EU. It puts new obligations on anyone who handles EU-based personal data.

To ensure that all our services and product features meet the data protection standards required of data processors by the GDPR, Agiloft has reviewed and audited its security technologies and privacy policies and confirms it is compliant with GDPR.

Security has always been our highest priority, and we continue to review, develop, and test our products and services to ensure that we adhere to the highest security and data protection standards.

GDPR Overview

The GDPR replaces most of the varied national data protection laws that have been used by the different countries in the EU with a single set of rules. Companies with a business presence in the EU who process personal data must meet the requirements of the GDPR. This also includes businesses that may not be physically located in the EU but sell goods and/or services to or track the data of EU citizens. Additionally, the GDPR extends to non-EU citizens who have their personal data collected in the EU.

Here are the key points to know about the GDPR:

- **The GDPR applies to all personal data for people in the EU.** It is not tied to nationality. An American citizen in the EU is covered. A German citizen residing in the USA is not covered for data collected and used in the USA.
- **The GDPR does not replace Privacy Shield.** Privacy Shield covers data transferred across EU borders. GDPR covers a person's EU rights to know about data collected about them and to manage its use. The GDPR gives EU residents a right to:
    - Access and rectify data about themselves
    - Demand erasure of that data unless there is a compelling reason to not do so
    - Put restrictions on the non-legitimate use of that data
- **You should not ignore the GDPR.** Even though EU customers and data may be a minor part of your business, you are under its jurisdiction. The GDPR specifies major penalties for non-compliance:
    - For non-compliance related to technical measures such as impact assessments, breach notifications and certifications, the fine can be up to an amount that is the greater of €10 million (~US $12.5M) or 2% of your global annual revenue from the prior year.
    - For non-compliance with key provisions, regulators have the authority to levy a fine in an amount that is up to the greater of €20 million (~US $25M) or 4% of global annual revenue for the prior year. Examples that fall under this category include the transfer of personal data to third countries or to organizations that do not provide an adequate level of data protection.

Companies are responsible for assessing the scope of the GDPR within their own organization and taking the steps necessary to ensure compliance.

Key Terminology

GDPR makes a key distinction between a "Data Controller" and "Data Processor."

Data Controller

The data controller is "the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data."

Since our customers determine and control the collection and use of all data on their Agiloft systems, they are Data Controllers under the GDPR definition.

Data Processor

The data processor is "a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller." For customers that are hosted on Agiloft servers, Agiloft is the Data Processor of the data they have in Agiloft. Customers that host Agiloft on their own server are their own Data Processor.

Data Protection Authority

This is the authority that enforces the GDPR. It is a part of the national government for every country in the EU. In Germany it is different for every state.

Key Documentation Needed for GDPR

Data Controllers under the jurisdiction of the GDPR must have the following documentation to manage their data protection obligations and to show evidence of their active responsibility for that data.

Data Processing Addendum (DPA)

Article 28 of the GDPR states: "Where processing is to be carried out on behalf of a controller, the controller shall use only processors providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that processing will meet the requirements of this Regulation and ensure the protection of the rights of the data subject.

The processor shall not engage another processor without prior specific or general written authorisation of the controller."

The written description of what the data processor must guarantee is given in a DPA document that is signed by the Data Controller and the Data Processor.

Data Privacy Impact Assessment (DPIA)

DPIAs are compulsory under the GDPR where a "type of processing in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operation on the protection of personal data".

A DPIA is a risk assessment of the proposed processing of personal data. If your company is processing personal data that is likely to result in a substantial risk to the data subject's rights, a DPIA

must be carried out prior to commencing that processing. It must be made available to the Data Protection Authority if requested in response to a data privacy complaint under GDPR.

Article 30 reports

Article 30 of the GDPR states "Each controller and, when applicable, the controller's representative, shall maintain a record of processing activities under its responsibility." A company that receives a data privacy complaint under GDPR must provide an Article 30 report to the relevant Data Protection Authority. There is no set format for an Article 30 report.

Data Privacy Rights Granted by the GDPR

The regulations of the GDPR are centered around eight fundamental rights that EU residents have over their data. Your internal processes and systems will need to accommodate them. They are:

1. **The right to be informed**– You need to publish your privacy policies and intentions for people's data in plain language that is easily understood. Additionally, you need to be able to answer questions from customers and employees about how you use their data.
2. **The right of access**– You need to ensure that if a customer or employee requests a copy of the data you hold about them, you can provide it in a commonly used electronic format, for free, within a month of receipt of the request.

3. **The right to rectification**– If an individual believes that you hold incorrect or incomplete information about them, they're entitled to have that information corrected.
4. **The "right to be forgotten"**– An individual has the right to have their personally identifiable information deleted from your systems upon request.
5. **The right to restrict processing**– Individuals can object to you processing their data for a certain task. If they do so, you can retain enough of their data to ensure that their request is met.
6. **The right to data portability**– If a customer has willingly provided you with their data, they also have the right to request that it be transmitted to another organization should they so wish. For example, this might occur when a customer is changing service providers.
7. **The right to object**– Customers and employees have the right to object to processing and direct marketing of their personal data, including the right to retract previously given consent.
8. **Rights regarding automated decision making and profiling**– This protects people from potentially damaging decisions being made without human intervention.

Most important is the matter of consent; individuals will need to specifically consent to companies using and storing their details for any use, including marketing, analysis, or sharing with third parties. You cannot use an "opt out" scheme. This applies to EU customers you already have, not just new ones. Full, knowing consent must be sought from individuals before any further marketing actions can be made to them.

The Agiloft platform and the GDPR

Many requirements under the GDPR focus on ensuring effective control and protection of personal data. Agiloft gives you the capability to implement your own security measures that you need to enable your compliance with the GDPR, including specific measures such as:

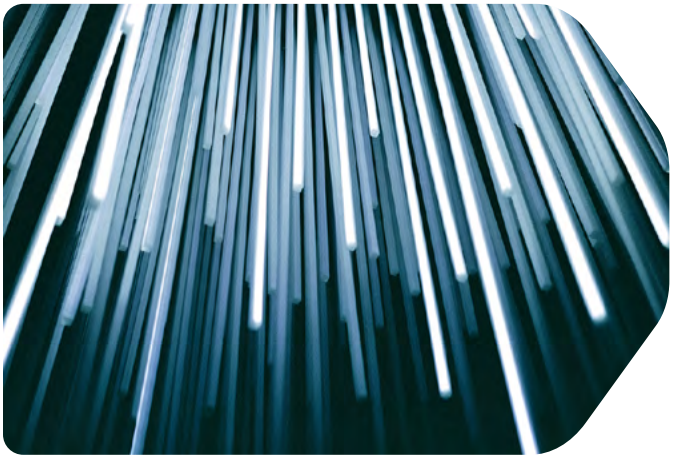
- Data Protection– Agiloft is designed for full data protection. You can configure access, including full password controls, using LDAP, two-factor authentication, and other industry-standard security protocols. All data and actions in Agiloft can be controlled by permissions down to the data element level to allow different abilities to create, modify, and view data by roles and group permissions.
- Data Process Auditing– Agiloft maintains a configurable audit trail, or history mechanism, of all data additions, deletions, and changes made.
- Secure Data Transmission– All data connections to and from Agiloft are encrypted.
- Data redundancy– Agiloft allows you to manage the creation of backups that contain all the data in Agiloft, not just the data in the database.
- Data portability– All data in Agiloft can be exported in a standard XML format.

Agiloft SaaS and the GDPR

Customers who have their Agiloft system hosted by Agiloft also benefit from additional data security and protection measures that are relevant to the GDPR:

- Encryption of personal data- All data on Agiloft servers is encrypted at rest.
- Data redundancy and data retention– Agiloft automatically maintains redundant sets of your data for 30 days.
- Restore access to data in a timely manner- Agiloft maintains redundant data stores for all your data. These can be retrieved in short notice. In the case of a hardware failure, Agiloft's systems will failover to a backup server in a matter of minutes.
- Regular assessment of processes- Agiloft regularly assesses and tests the effectiveness of our technical and organizational processes to ensure the security of your data and its processing.
- Centralized monitoring- Agiloft maintains continuous and centralized monitoring to identify potential intrusions and to monitor all equipment against failure.

- Data Removal– Agiloft can remove all traces of an individual's data not just from the database, but from all log and history files.
- Certified cloud providers– Agiloft uses both Amazon Web Services (AWS) and vXchnge as cloud providers.
- AWS provides compliance with rigorous international standards, such as ISO 27001 for technical measures, ISO 27017 for cloud security, ISO 27018 for cloud privacy, SOC 1, SOC 2 and SOC 3, PCI DSS Level 1, and EU-specific certifications such as BSI's Common Cloud Computing Controls Catalogue (C5).
- vXchnge provides compliance with SSAE 18, SOC 2 Type II, ISO/IEC 27001:201, and HIPAA/HITECH.



What Do You Need to Do?

You should consider the following areas in preparation for GDPR compliance:

- Determine whether the GDPR applies to your company's use of Agiloft.
- If you are subject to the GDPR, you will need to make sure you can meet the rights of data subjects whose personal data you control.
- If you are a data controller, you must report data breaches to the data protection authorities without undue delay and within 72 hours of you becoming aware of a data breach.
- If Agiloft detects a data breach it will inform all affected customers within 48 hours of our detection of the breach.
- If you are under the jurisdiction of the GDPR, you will need to have a data protection impact assessment (DPIA), and you might be asked for such documents by the GDPR supervisory authority. You should also appoint a Data Protection Officer (DPO) who will manage data security and other issues related to the processing of personal data.
- If Agiloft is hosting your Agiloft system and the GDPR applies to you in any way, you will need a data processing agreement (DPA) that meets the requirements of the GDPR; particularly if personal data is transferred outside the European Economic Area.
    - Agiloft offers a GDPR-compliant Data Processing Addendum (DPA), enabling you to meet the GDPR requirements for agreements between you, as a Data Controller, and Agiloft, as a Data Processor.

FAQ

What is the GDPR?

The GDPR is a new comprehensive data protection law that takes effect May 25, 2018 in the EU. It strengthens the protection of personal data and backs up that protection with the potential for very heavy fines against companies that violate its provisions, up to the greater of €20 million (~US $25M) or 4% of global annual revenue for the prior year.

What does the GDPR cover?

The GDPR regulates the "processing" of personal data collected in the EU, which includes collection, storage, transfer, or use. Any organization that processes personal data collected in the EU is covered by the law, even if the the company does not have a physical presence in the EU. The GDPR, defines "personal data" very broadly. It covers any information relating to an identifiable individual. This includes, but is not restricted to, name, address, identification numbers, email address, phone number, photos, etc.

How does GDPR change privacy law?

The GDPR significantly expands data privacy rights for personal data collected in the EU. It replaces the patchwork of national privacy laws within the EU with a single set of rules and provides centralized enforcement by requiring companies to work with a lead supervisory authority on cross-border data protection.

Is personal data required to stay in the EU?

No, the GDPR does not require EU personal data to stay in the EU, nor does it place any new restrictions on transfers of personal data outside the EU. The rules for transfer of data across EU boundaries to and from the USA is covered by the Privacy Shield Framework, of which Agiloft is a member.

Where can I learn more about the GDPR?

There are several good websites that will give you more information about the GDPR:

- The EU's official GDPR website
- The UK's Information Commissioner's Office GDPR website
- The Full Text of the GDPR
- TrustArc's GDPR Priorities Assessment

About Agiloft, Inc.

As the global leader in agile contract lifecycle management (CLM) software, Agiloft is trusted to provide significant savings in purchasing, enable more efficient legal operations, and accelerate sales cycles, all while drastically lowering compliance risk. Agiloft's adaptable no-code platform ensures rapid deployment and a fully extensible system. Using contracts as the core system of commercial record, Agiloft's CLM software leverages AI to improve contract management for legal departments, procurement, and sales operations. Visit www.agiloft.com for more.

Agiloft, Inc. | 460 Seaport Court, Suite 200 | Redwood City, CA 94063 | 650-587-8615 | 1-888-727-2209 | info@agiloft.com | www.agiloft.com