PRONTO
SOFTWARE

GDPR

What you need to know about the European General Data Protection Regulation

The European Union has taken steps to protect the fundamental right to privacy of every EU resident with the introduction of the General Data Protection Regulation which takes effect from 25 May, 2018.

European Union (EU) residents will now have greater say over their personal data; how it is used, processed or deleted. This rule clarifies how the EU personal data laws apply, even beyond the borders of the EU. Any organisation that works with EU residents' personal data - irrespective of location - has obligations to protect related data. To review detailed definitions and articles, go to European Union's website.

Key Definitions

What is personal data?

Any information related to a natural person or 'Data Subject' that can be used to directly or indirectly identify the person. It can be anything from a name, a photo, an email address, bank details, posts on social networking websites, medical information, or a computer IP address.

Who is a data controller?

A controller is the entity that determines the purposes, conditions and means of processing the personal data.

Who is a data processor?

The processor is an entity that processes personal data on behalf of the controller. Pronto Software is addressing GDPR requirements as a data processor on our customers' behalf who are the data controllers.

Key Considerations

Increased Territorial Scope (extra-territorial applicability)

General Data Protection Regulation (GDPR) applies to the processing of EU citizens' personal data by the data controller and data processor, regardless of where the data controller or data processor are located.

Data breach notification

A mandatory breach notification must be made by data controllers within 72 hours of first becoming aware of it in all member states where the data breach is likely to "result in a risk for the rights and freedoms of individuals." Data processors are also required to notify their customers, the controllers.

Right to access

The right of data subjects to obtain confirmation from the data controller as to whether or not personal data concerning them is being processed, where and for what purpose. The controller shall provide a copy of the personal data, free of charge, in an electronic format.

Right to be forgotten

The data subject is entitled to have the data controller erase his/her personal data, cease further dissemination of the data and potentially have third parties halt processing of the data. Data portability GDPR introduces data portability - the right for a data subject to receive the personal data concerning them from a controller and transmit it to another controller.

Privacy by design

Privacy by design calls for the inclusion of data protection from the onset of the designing of systems, rather than an addition. For example:

- Controllers must implement appropriate technical and organisational measures in order to meet the requirements of this Regulation and protect the rights of data subjects
- Controllers must hold and process only the data absolutely necessary for the completion of its duties (data minimisation), as well as limiting the access to personal data to those performing the processing.

Data Protection Officers

To meet GDPR internal record keeping requirements, the appointment of a Data Protection Officer (DPO) will be mandatory for those controllers and processors whose core activities consist of processing operations which require regular and systematic monitoring of data subjects on a large scale – or of special categories of data, or data relating to criminal convictions and offences

How will Pronto Software help your organisation comply with GDPR?

Tips to prepare for GDPR as a data controller:

1. Familiarise yourself with the new regulation
2. Assess whether it is necessary to appoint a Data Protection Officer (DPO)
3. Review and enhance your current processes for storage and use of personal data
4. Establish procedures to respond to data subjects when they exercise their rights
5. Establish procedures for data breach notification
6. Raise employee awareness on GDPR compliance

Commitment to data security and Compliance

As an organisation, Pronto Software and all subsidiaries are contractually obligated to observe the principles of the Australian Privacy Act including the recent changes via the Notifiable Data Breach (NDB) scheme. The introduction of GDPR however extends the European Union's reach to Australian organisations who hold the personal information of EU residents.

Pronto Software is investing heavily in the area of security, risk and compliance through a formal "Security, Risk and Compliance" governance structure that reports directly to the Pronto Software board.

Pronto Software will continue to be committed to safeguarding the security of its customer solutions to ensure it remains compliant with applicable legislations.

Pronto Cloud

Pronto Cloud is undertaking the ASAE3402 compliance audit which provides independent assurance reports on our controls as a service organisation. As part of the compliance program, a set of minimum baseline IT general controls have been established which covers the protection and security of customer data. The key components of our ASAE3402 controls are information security awareness, logical and physical access security, security measures to counter malicious electronic attacks, encryption, backup and recovery, change management, as well as sub-processor/ third-party management.

In addition, Pronto Cloud undertakes annual penetration testing which is conducted by a third party security specialist to specifically undertake both internal and external network testing. The main aim of this testing it to stress test the environment to discover any potential vulnerabilities that may need to be remediated and to implement improvements to our overall security posture.

We also have an ongoing project in relation to aligning Pronto Software to the ISO 22301 standard for "Business Continuity" to ensure that we have managed our risk effectively and have all relevant procedures and documentation in place to recover our systems and customers within Pronto Software, in the event of a breach or disaster.

Breach notification

Pronto Software already has an established Incident Management system in place and we have updated our policies and procedure as a data processor, to comply with GDPR. As part of that procedure, we will promptly notify relevant regulators and the customer, the data controller, after becoming aware of a data breach.

Right to access

As a data processor, we will assist customers with responding to individual rights requests that they receive under the GDPR. In many cases, customers may be able address these types of requests by performing their own data management within the applicable Pronto Software application(s) and tools.

Right to be forgotten

As a data processor, we will assist the customers, the data controller, with erasing individual personal data and cease further dissemination of the data from the hosting infrastructure.

Data portability

GDPR gives end users the right to either receive all of the data provided and processed by the controller or transfer it to another controller depending on technical feasibility. As a data processor, we will further enhance the robustness of our capabilities to export data at an individual level.

Privacy by design

At Pronto Software, we employ a least-privilege-access principle. Only a limited number of roles within Pronto Software are authorised to access customer environments and only when necessary, according to guidelines. As a data processor, we only process customer data according to the customer's instructions.

For Pronto Cloud customers, we require any sub-processors that handle personal data, including our data centre partner, to follow the same security and privacy standards we adhere to. We store data in data centres located in Australia that are ISO 27001 and ISO14001 certified. Pronto Cloud employs various security measures to protect customer data such as multifactor authentication, firewall, antivirus, patching, encryption in transit and encryption at rest, vulnerability scanning, Intrusion Detection (IDS), Intrusion Prevention (IPS) and log security event management (SEM). We have various monitoring systems in place that pulse check our entire environment covering our network, physical hardware and our virtualised platform. Our systems are monitored 24/7/365 with automated alert notifications to engineers.

Data Protection Officer

Pronto Software is in the process of appointing a dedicated Data Protection Officer. In the meantime, if you have any privacy policy questions or concerns relating to your information, please contact us via email to privacyofficer@pronto.net or by writing to:

Privacy Officer
Pronto Software Limited
20 Lakeside Drive,
Burwood East, Vic 3151
Australia