Whitepaper

INFINIGATE
.... Adding Value to Distribution

GDPR Checklist:
11 Step Plan for the Incoming Regulation

Have you started your preparations for the GDPR (General Data Protection Regulation)?

Even the strongest of ignorance couldn't fail to relent against the torrent of information available, from the predicted doomsday penalties, to the deafening tick of the countdown clock, there is no abate. For most IT administrators, the journey to compliance has yet to begin for the simple reason...where to start?

To help with the road ahead, we have simplified the regulation to eleven steps which cover crucial areas of the GDPR and how you should prepare for them.

1. Raise Awareness

The GDPR is likely to enforce some moderate to significant changes in the way that your organisation collects and processes data. Although a successor to The Data Protection Act 1998 and encompassing many of its existing provisions, the GDPR packs more of a bite and therefore will need to be adhered to more carefully.

There are two distinct audiences which will need to be educated about the incoming changes. The decision makers of the organisation will need to have understood the reasons for compliance and what the journey to compliance involves. In addition your wider staff cohort will need to be briefed about changes to the way they work, particularly if they handle personal data. Staff members who handle personal data are operators of your data processors and will be adhering to the regulation every day.

2. Perform a Data Audit

The main focus of the GDPR is protecting the digital rights of individuals whom are referred to as data subjects. All personal data collected from data subjects should be audited and documented to ascertain what is being held and for what purpose.

Note that the supervisory body for an EU member state (in the case of the UK is the Information Commissioners Office) has the legal entitlement to request this documentation from any organisation whose business is conducted in their jurisdiction.

3. Communicate Clearly to Data Subjects

The days of ambiguous terms and conditions when submitting forms is coming to an end. The GDPR specifies that data subjects should be made aware, in clear language, why their personal data is being collected, for what purpose and how long it will be stored for. Data subjects must explicitly opt-in and accept these conditions with the burden of proof now being placed on the collector.

Review all points of data collection, including paper based forms, as the GDPR covers anything which becomes part of a filing system in an automated system.

4. Consider the Purpose of Data Collection

The GDPR makes no exception when it comes to the boundaries of what is and what isn't acceptable when collecting personal data. Organisations are legally required to justify why each item of personal data is collected and to collect no more than what is absolutely required. Personal data that has been collected can only be held for the length of time which it is needed, with indefinite not being an option.

Liaise with the various departments of the organisation to understand what personal data has been collected and whether or not it is strictly required. Also consider how personal data is processed for deletion and whether it carries an expiration date.

5. Understand Data Subjects Rights

Much like under The Data Protection Act 1998, data subjects have a right to request access to personal data related to them of which you are storing or processing. The time frame to comply has been reduced from 40 to 30 days and administration fees have been abolished.

In addition, the GDPR hands more power to data subjects who can now request that personal data is rectified if incorrect, have data erased, prevent marketing and prevent profiling.

Think about your organisation's processes and workflows for carrying out each of these functions; understand that the GDPR requires these functions to be easily accessible to data subjects in a manner similar to the way in which they submitted personal data.

6. Provide Data Portability

Possibly the most interesting inclusion of all the data subject rights is the one that requires data controllers to provide data subjects with the means to move their personal data between controllers. This can be provided in two ways; an exported format which should be readable to any other controller, or an automated means of transferring data between controllers without the data subject being an intermediary. This is much like the process of moving between home utility companies or mobile telephone contracts.

This is likely to be a new and unexplored requirement for most organisations and conversations with other organisations within the same industry should be happening now to form a common framework for data portability.

7. Conduct Data Protection Impact Assessments

In scenarios where data processing is likely to result in a high level of risk to the data subject's rights, the GDPR mandates that data controllers perform a data protection impact assessment (DPIA). Well prepared organisations, or even those who have already been through risk assessment programmes in the past, may be able to transfer most of this information from their existing risk registers.

The definition of what constitutes a high level of risk is determined by the supervisory authority (e.g the Information Commissioners Office in the UK) and what is yet to be fully clarified. However, it is prudent that you use your own judgement until full guidance has been provided. Penalties can be applied should an organisation be found not to have documented the risks to the data subject's rights.

8. Adhere to Data Processing Systems and Security by Design

When designing data processing systems or simply as a result of DPIAs, the confidentiality, integrity and availability of those systems must be guaranteed and documented. Provisions for security by design has been included in the GDPR to mitigate against security controls being implemented post-incident and to focus instead on prevention by default. For example, is personal data stored in a database in a non-encrypted format and therefore susceptible to being read by unauthorised parties? This should be addressed by some form of encryption or other data obfuscation method.

Investigate all known automated data processors and document the steps taken to ensure a high level of confidentiality, integrity and availability for those systems. Performing this gap analysis will highlight areas of high risk.

9. Create or Refine Reactive Policies

Incidents of data breach, manipulation and destruction will no longer be something which you can choose whether or not to disclose. The GDPR now requires the disclosure of such incidents to the supervisory authority within 72 hours of the data controller becoming aware. In the most severe cases the data controller is compelled to notify the data subjects individually with information such as what the incident is, which personal data items are affected and how the controller proposes to address the incident.

Ensure you have policies and processes implemented for such scenarios with contact information of the supervisory authority, sufficient logging, investigation tools and template messaging for both the supervisory authority and the data subject available.

Much has been made of the monetary penalties available under the GDPR and whether or not you should brief your board and decision makers about the potential values. There are two tiers of penalty available dependant on which areas of the regulation are violated, each with a maximum value. In addition to this the data subjects themselves have the right to seek damage claims against data controllers during instances where they are put at risk.

W: www.infinigate.co.uk | T: 0845 4900 245 | E: marketing@infinigate.co.uk

10. Have a Point of Contact

Openness and fairness are words frequently mentioned throughout the GDPRs pages in relation to the accessibility of communication channels for data subjects to data controllers. All data controllers must provide contact details of a member of their organisation who can be contacted by data subjects to exercise their data subject rights. This must be done easily and in a way which best represents how the personal data was submitted. e.g if by phone, the phone number of a representative must be provided.

Nominate a data control contact point for your organisation and publish their contact details on all points of data collection and to the supervisory authority.

For organisations who are public authorities, such as local councils or police forces, or those which process significant quantities of personal data, a Data Protection Officer (DPO) will need to be appointed. A DPO takes the point of contact role one step further and acts as a responsible party in all cases of data processing. The GDPR specifies that this person need not be an employee of the organisation and need not be available on a full time basis but should be involved in all cases where data processing is modified, assessed or implemented. If required, hire or nominate a DPO. Note that the DPO is defined as being suitable for the role and cannot be assigned to someone just for the need to quickly comply.

11. Get Accredited

Although untested and tenuously referred to, the GDPR recommends that supervisory bodies develop accreditation for GDPR compliance, and offers leniency for scenarios where data controllers or processors have recognised information security accreditations.

Consider implementing internal standards for information security such as ISO27001, much of the GDPR is aligned with the well-known standard and this will make the regulation much less of a leap into the unknown.

The GDPR was created not to be a tick box exercise but to force organisations to review themselves as data controllers & processors. Controls implemented are based on risk & gap analysis and not by way of mandated technology. As a result there is no such thing as a GDPR silver bullet, however the steps outlined above are a good starting point.

The journey to GDPR compliance is long, arduous & likely to contain unanticipated twists & turns. However, it is a path which all organisations must walk, some more reluctantly than others.

As of May 2018 the ICO will show it means business, gaining renewed focus after two decades of enforcing an ever increasingly obsolete data protection law. Act now to avoid the cross hairs; time available now offers you more breathing space than when the GDPR comes into effect.

W: www.infinigate.co.uk | T: 0845 4900 245 | E: marketing@infinigate.co.uk

This article was written by Chris Payne, Senior Technical Consultant at Infinigate UK. With 9 years of experience working in IT security, Chris has a wealth of knowledge around information security and holds a GDPR certification under IBITG. In addition to this, Chris has worked on some of Infinigate's largest ever deployment projects and regularly appears as a guest contributor to IT security related blogs, whitepapers and articles.

About Infinigate UK

Infinigate is a leading Value Added Distributor (VAD) of IT security solutions in Europe. Infinigate was founded in 1996 and has today 8 subsidiaries. Infinigate offers state-of-the-art IT Security solutions through its European partner network (VARs, integrators, consulting companies, etc.) to secure and protect IT networks and data. Infinigate provide the following solutions:

- Data Loss Prevention
- Digital Forensics
- Endpoint Security
- Identity & Access Management
- Mobile Security
- Network Management & Security
- Web & Email Security