GDPR Compliance at Criterion IT Ltd

Purpose

This document is primarily intended for customers. Some customers have asked us to communicate to them what we have done to prepare for GDPR, and we anticipate there may be more such requests. So this document sets out to:

- Explain how we as a company have approached the challenge of GDPR.

- Outline practical steps we have taken or are taking in direct response to the stipulations of GDPR.

- Explain decisions we have made in terms of how we handle data – since, as we understand its intent, GDPR is a set of guiding principles that each organisation must interpret and put into operation according to its own context.

May 2018
Version 1.0

Overview

We began to investigate the implications of GDPR for our business in a serious root and branch fashion early in 2017. At that time there was a growing number of 'scare stories' emerging about GDPR - especially relating to the fines in the event of a data breach. And a lot of companies were trying to make a fast buck out of GDPR, which didn't help to make things clearer.

However, it was also clear to us that doing nothing was not an option. The issue was regularly discussed at monthly executive management meetings and we felt it was important to take considered action since:

- It is vital for us from a commercial perspective to retain the trust and confidence of our customers.

- Our business philosophy is based on identifying and implementing planned and repeatable processes. We saw GDPR as an opportunity to extend these.

- As a company with approaching 20 employees, it is important for our growing reputation for Criterion to continue to act responsibly and be seen to act responsibly within the diverse communities in which we operate.

- We have never positioned ourselves externally as a GDPR expert but we do sell business continuity and data security solutions (which could form part of a GDPR solution). To a certain extent we feel an obligation to lead by example in terms of implementing best practice.

As a company, Criterion has taken GDPR extremely seriously. We have done our very best to ensure our systems and processes are compliant.

To that end, some members of staff have attended a GDPR workshop run by a certified external consultant.

We are also making stringent efforts to ensure every member of our staff has been made aware of the principles of GDPR and how it might affect their job role. We are carrying out training before implementation on 25th May 2018 and then planning to run regular refresher sessions after GDPR comes into force.

Our Senior Management are committed to ensuring that everyone within the company is aware of their responsibilities under GDPR. Whether you are an engineer, salesperson or administrator, you are likely to have some interaction with our customers. It is therefore important everyone has a sound grasp of the core principles of GDPR.

GDPR Implications for Criterion

Looked at pragmatically, GDPR is a set of guiding principles, particularly with regards to PII (Personally Identifiable Information). There are no hard and fast definitions of what to do. Instead, every company must undertake its own risk assessment, make its own decisions in line with GDPR principles and ensure appropriate processes are in place. In the case of Criterion, those decisions will be taken by the joint Copyrite/Criterion GDPR committee and ultimately signed off by our MDs.

At its core, GDPR is a shift in mind-set. It essentially updates data protection for the digital age. If you like, it involves everyone within Criterion learning to 'stand in the individual's shoes' and think deeply and seriously about what they do with personal data. That's why we believe the training aspect is so important.

Our investment of time and energy in the GDPR compliance process has led us to these insights and conclusions:

- GDPR is not specific to one part of our business. Its implications potentially touch marketing, HR, sales, finance, support, systems and IT. So we have brought together a multi-disciplinary team that can take a holistic approach.

- We already have many robust processes in place. For example, if something goes wrong, we have defined processes in place that define what should happen and how. We have worked to ensure these processes are aligned with the requirements of GDPR, especially where GDPR brings into being new processes.

- Building on this GDPR has led us to introduce new processes - for example, the right to be forgotten. We have taken appropriate measures to support these new processes.

- GDPR stipulates that, for data that is held, adequate measures must be implemented to prevent personal data from being stolen, lost or subject to unauthorised access. Criterion as a matter of policy stores all data in a private cloud that is dedicated to Criterion and not shared with anyone else. The data centre holding the data itself is certified to ISO 27001 standard. Data is backed up on a nightly basis via a dedicated private fibre network to a remote location. In terms of this data backup process, data is encrypted both in transit and at rest.

- As part of our preparatory work for GDPR, we have reviewed the data sets we store across the company. Much of our operational data is at the company level and does not identify individuals within an organisation. For example, we store data about printers and their usage, but in terms of identifying individuals this data is aggregated and anonymous. Our help desk logs support calls but, again, these are recorded at the company level.

- We do hold data on our customers, notably in our CRM system. For the most part, we hold very limited information - typically, customer's name, job title and contact details.

- We carry out corporate hospitality and for that reason we identify any known interests of some individuals. For example, if we know that Customer A is a rugby fan, we might record this on the CRM and use this when we run a hospitality event at a rugby match. We believe this is a legitimate business use of personal identifiable information.

- We use contact information on our CRM to communicate with our customers by email, sent to a work email address provided by the customer. These e-mails provide those customers with relevant information about new services and upgrades that we have added to our portfolio. This activity is vital to the continued growth and development of our business and we therefore regard it as necessary to our business. We understand that the ICO (Information Commissioner's Office) makes provision for this kind of activity which it refers to as the soft opt-in:

    1 "Organisations must not send marketing texts or emails to individuals without their specific prior consent. There is a limited exception for previous customers, known as the soft opt-in." (Source: ICO Guidance on Direct Marketing, version 2.2)

- Customers can easily and conveniently opt out of email communications at any stage, and we have taken steps to tighten this process and make it easier and quicker to opt out.

- As part of our data audit, we have also discovered that, in the past, enthusiastic sales people have added information to the CRM about their customers, including marital status and family members. Historically, this has been fairly standard practice within our industry, but does not seem to align with the principles of GDPR. We have therefore decided this is not a legitimate business use of personal identifiable information and we are currently in the process of removing and deleting such data.

- Certain aspects of GDPR do not apply to Criterion. For example, we do not do any processing of data outside the UK. Nor do we undertake any data profiling activity to identify the habits and tastes of a person. And we do not store data about young people that might require parental consent (the only data we store relating to schools concerns the contact details of relevant staff at schools that are Criterion customers or prospects).

The members of the joint Copyrite/Criterion GDPR team are currently:

Victoria Ford, Company Secretary and Data Protection Officer
Diane Littlecott, Operations Director
Mike Burden, IT Director
John Grey, Project/Process Co-Ordinator

This team meets on at least a monthly basis.

Appendix: Our Understanding of GDPR

The General Data Protection Regulation (GDPR) is enforceable from 25th May 2018. Its purpose is to provide a modernised accountability-based framework for data protection that will replace the preceding DPA (Data Protection Act 1998).

Categorisation of personal data needs to be established and maintained as a natural integrated part for how processes are established and performed. The concept can be judged using three principles:

- Purpose Limitation
- Minimisation
- Storage Limitation

Need-Want-Drop

Purpose Limitation from the Data Subject's perspective	
NEED	**WANT**
Essential Information without this you cannot perform the task or service	Non-essential Information that is useful/profitable to the business

The above applies to all data pre- and post-processing i.e. input, output and retained archives or backups cycles.

Whilst categorising the PII data that is held-used, data controllers and processors need to cater for 3 of the total 8 rights of the data subject:

- The right to be forgotten
- The right to object
- The right to withdraw consent at any time

For data that is held, adequate measures must be implemented to prevent personal data from being stolen, lost or subject to unauthorised use. This includes equipment and mobile devices used. The Information Commissioner has formed the view that in future, where losses occur and where encryption software has not been used to protect the data, regulatory action may be pursued.

When transferring data, a controller may only transfer personal data outside the EEA to a country whose data protection laws have been approved by the European Commission as providing adequate protection for data subjects' rights.

The adequacy of the level of protection associated with a transfer may be ensured in a number of ways. The data controller may:

- carry out his/her own assessment of the adequacy of the protection
- use contracts to ensure adequacy
- obtain Commission approval for a set of Binding Corporate Rules governing intra-group data transfers
- rely on one of the exceptions to the prohibitions on transfers of personal data outside the EEA.

Destruction or deletion, as best practice, organisations should ensure when personal data is deleted, the deletion is irretrievable and not simply deactivated or archived. If you offer users the option to delete personally identifiable information uploaded by them, the deletion must be real i.e. the content should not be recoverable in any way. It is bad practice to give a user the impression that a deletion is absolute, when in fact it is not. The same care applies for data housekeeping in relation to storage limitation and the destruction of disused equipment and storage media.

Data Protection Impact Assessment (DPIA), it is important to recognise when an DPIA should be conducted. DPIA is a structured process that should be used to identify and reduce risk which may lead to a data breach. An DPIA should be considered when either of the following are recognized, being planned, designed or implemented:

- new processes
- changes to existing processes
- enactment of any data subject rights being requested
- identified data breach

Principles and Rights

There are 7 principles and 8 rights that are the focus of GDPR:

Principles	**Rights**
Legality, Transparency & Fairness	The right to be informed
Purpose Limitation	The right of access
Minimisation	The right to rectification
Accuracy	The right to erasure
Storage Limitation	The right to restrict processing
Integrity & Confidentiality	The right to data portability
Accountability	The right to object
	Rights in relation to automated decision making and profiling

Lawfulness of Processing

The following list conditions where the rights of the data subject may be outweighed:

1. Consent of the Data Subject
2. Processing is required for the performance of a contract with the Data Subject or to move towards entering into a contract
3. Legal obligation
4. To safeguard the vital interests of a Data Subject
5. Where processing is required to be carry out in the Public interest or in exercise of an official authority vested in the Controller
6. Necessary to legitimate interests pursued by the Controller or a third party, except where such interests are outweighed by the interests, rights or freedoms of the Data Subject
7. Processing is required for carrying out obligations under employment, social security or social protection law, or a collective agreement
8. Processing is required to protect the vital interests of the Data Subject where the Data Subject is legally or physically unable to give consent

Compliance framework

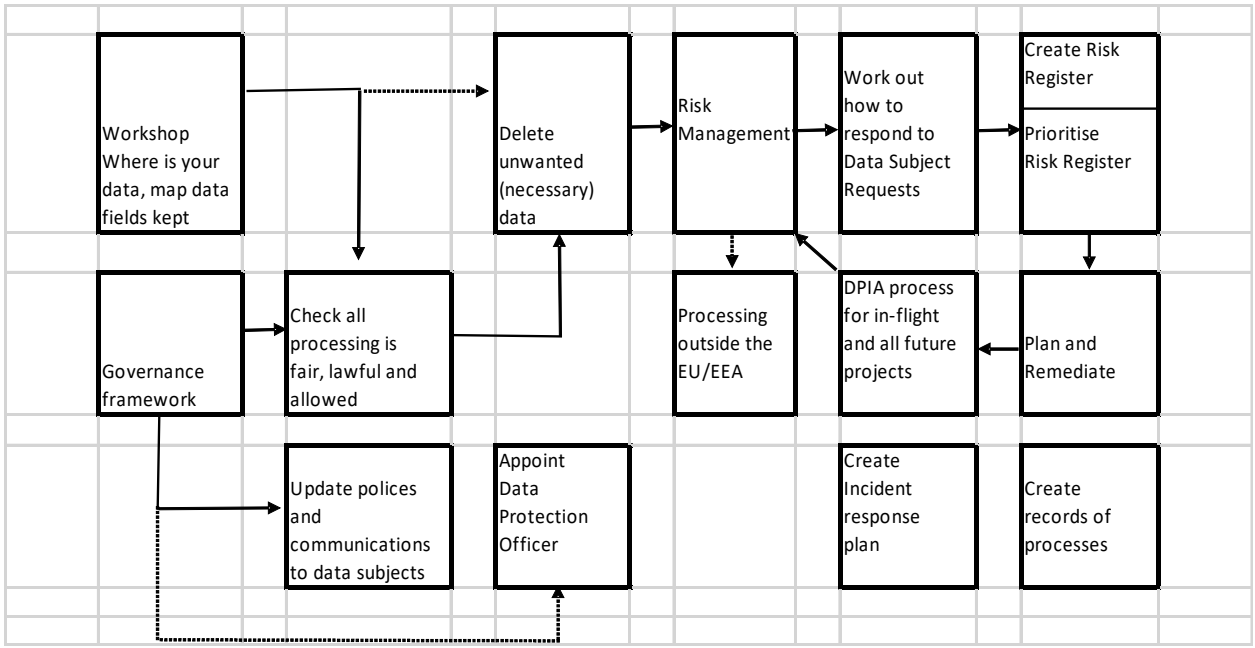
There are several compliance frameworks that can be used in conjunction with GDPR, however there are only two officially recognized standards:

- ISO/IEC27001:2013
- BS10012:2017

Regardless of the chosen compliance framework used, the following lists key areas for privacy compliance are:

- Organisational privacy policies and principles
- Risk management
- Incident management
- Change management
- Continual improvement

The following is a road map that illustrates the broad approach that Criterion has adopted to identify and address what needs to be done in preparation for GDPR compliance and also the ongoing activities that need to become adopted as part of the ongoing company practices and policies.


Workshop
Where is your data, map data fields kept
Delete unwanted (necessary) data
Risk Management
Work out how to respond to Data Subject Requests
Create Risk Register
Prioritise Risk Register
Governance framework
Check all processing is fair, lawful and allowed
Processing outside the EU/EEA
DPIA process for in-flight and all future projects
Plan and Remediate
Update polices and communications to data subjects
Appoint Data Protection Officer
Create Incident response plan
Create records of processes

•