Simple Business GDPR Information Security Guidance

Introduction

There are plenty of Cyber Security Sales and Marketing teams jumping on the General Data Protection Regulation (GDPR) bandwagon at the moment, often peddling fear of massive penalty fines and in far too many cases spouting nonsense and unnecessary guesswork about the GDPR's information security requirements.

You do not need to be a lawyer or a fancy pants security consultant to understand the GDPR's information security requirements, they are freely provided by the European Union. It is just a matter of taking the time to actually read and digest each of the GDPR's requirements and then interpreting how your organisation will comply, albeit some requirements may result in full blown project plans. I recommend reading the bite-sized formatted and section headed version of the GDPR on **www.privacy-regulation.eu/en/** rather than the **EU released GDPR paper.**

Everything in this article is not official legal advice but an interpretation and personal opinion on meeting the GDPR's information security requirements. Further official and detailed GDPR Information Security guidance are expected to be released.

Brexit

The United Kingdom's exit from the European Union will not occur before GDPR comes into UK law on 25th May 2018. Therefore all UK organisations storing or processing any personal data records will have to comply with the GDPR from May 2018. It is highly likely GDPR compliance will continue to be a UK personal data legal requirement post Brexit. The GDPR applies to any non-EU country processing EU Citizen personal data; it is unlikely the UK will adopt a tiered data protection legal requirements system, where UK nationals have fewer privacy rights than EU nations.

Only 3 of the 99 GDPR Requirements are directly InfoSec Related
That's right, there are just three information (data) security requirements in the GDPR, Articles 33, 34, and 35, the other 96 Articles relate to data subject rights, data controller responsibilities, sending personal data outside the EU and general administration. There is a hidden Information Security requirement in GDPR Recital 63, but aside from that, there is not a lot for information security professionals to worry about unless you have been tasked to prepare an organisation to meet all the GDPR's requirements, in which case you need to be a data privacy qualified.

Information Security Vs Data Privacy
Some companies like to lump data privacy within information security management, but to properly understand and manage modern data privacy rights in medium to large organisations, it requires individual(s) with the appropriate qualifications and background in privacy law. Data Privacy is a completely separate discipline, applying privacy rights intricacies within business processes can be completely alien to the average information security professional. We still live in an age where the information security function is incorrectly placed as a subset of IT in some organisations, but nether-the-less even though privacy and security are linked they should be regarded as separate business functions and as separate professions, a notion included as a requirement in the GDPR under Article 37.

Article 37 **"Designation of a Data Protection Officer"**
"*the data protection officer shall be designated on the basis of professional qualities and, in particular, expert knowledge of data protection law and practices and the ability to fulfil the tasks referred to in Article 39*."

Article 37 and Article 38 requires the designation of a Data Protection Officer (DPO)

Article 39 **"Tasks of a Data Protection Officer"** outlines a number of privacy officer duties, including monitoring compliance with the GDPR.

GDPR's Information Security Requirements

GDPR has 173 Recitals and 99 Articles. **Recitals** set out the reasons and what is trying to be achieved by the regulation, while **Articles** are the regulatory requirements, the GDPR rules.

Article 32 Apply Appropriate level of Information Security (Risk Assessed)

This is best practice Information Security Management, nothing specific or new here, it all should be already being done. Take a risk assessed approach, 101 information security; confidentiality, integrity and availability of all personal data within the organisation. Don't forget the availability as unlike PCI DSS the GDPR regards the availability of personal data as requirement. Article 32 requires information security to be of an industry best practice standard, appropriate to the size and nature of the organisation, this means information security does not need to achieve a 'state of the art' level but what a level that is generally considered an adequate level of security for the nature and type of organisation. So if your organisation already has a strong security posture, to the standard of ISO27001:2013, you are in an excellent position to meet GDPR information security requirements.

Article 33 Notification of Breaches to the ICO

The ability report data breaches to the ICO within 72 hours, so part of incident management and response policy and planning, include a process to inform the company designated Data Protection Officer (DPO) about any detected personal data breaches, allowing the DPO to be informed and to report any data breaches to the ICO.

Article 34 Notification of Breach to Data Subjects

As per article 33, ensure company DPO notification is included as part of your incident management/response process, to allow your DPO to inform data subjects should their personal data be at risk due to a security incident.

Article 35 – Data Protection Impact Assessment

"7. The assessment shall contain at least: (7d) ***the measures envisaged to address the risks****, including safeguards,* ***security measures and mechanisms to ensure the protection of personal data*** *and to* ***demonstrate compliance*** *with this Regulation taking into account the rights and legitimate interests of data subjects and other persons concerned."*

Article 35's 11 requirements is a Data Privacy Officer responsibility in my view so it is not concluded as one of the 3. However to meet some of Article 7d it cites a repeat of Article 32, a risk assessed approach to applying information security controls appropriate to protecting personal data.
Documentation and assessments evidence is required to demonstrate compliance, again such documentation and security assessments should already be in place if your organisation operates a best practice level information security management.

Privacy Articles References Information Security Requirements
Article 30 – Records of Processing Activities
"1. Each controller and, where applicable, the controller's representative, shall ***maintain a record of processing activities under its responsibility****. That record shall contain all of the following information.* ***g) where possible, a general description of the technical and organisational security measures*** *referred to in Article 32(1)."*

"2. Each processor and, where applicable, the processor's representative shall ***maintain a record of all categories of processing activities carried out on behalf of a controller****, containing* ***d) where possible, a general description of the technical and organisational security measures referred*** *to in Article 32(1).*

Another Data Privacy Officer set of requirements, but Article 30 references the Information Security "Article 32". In other words, make sure the record processing activities are in scope of the information security policy/programme, and the security controls are documented, which they already should be.

Data Subject Access Rights Portal
Recital 63 refers to organisations providing a Data Subject Access Rights Portal.
"Where possible, the controller should be able to provide remote access to a secure system which would provide the data subject with direct access to his or her personal data."
Providing a portal is "possible" for most organisations, for many organisations it could mean adding additional functionality to existing staff and customer facing websites/portals.
Bear in mind even though Recital 63 reads like a GDPR requirement, it is the Articles are the legal requirement to meet not Recitals. Then there is **Article 12** which states

"Where the data subject makes the request by electronic form means, the information shall be provided by electronic means".

The provision or expansion of an internet-connected portal to handle GDPR's data privacy rights could fulfil this requirement. Obviously, the privacy portal needs to be secure. As such it will be an information security responsibility and GDPR requirement to secure it.

GDPR Privacy Data Subject Rights (via an Internet Portal)
The GDPR requires the following data subject privacy rights to fulfilled within a one month and without any charge, so given Recital 63 and Article 12 the best way to do achieve this, especially where there are thousands of personal data records in the care of the organisation, is using internet facing portal to provide each data subject with the ability to exercise their new GDPR privacy rights.

- Article 13 - explain how personal data is processed
- Article 15 - provide a copy of personal data (Data Subject Access Request)
- Article 16 - correct any incorrect personal data
- Article 17 - personal data erasure
- Article 18 - restrict the processing of personal data
- Article 20 - personal data portability, provide personal data to another data controller
- Article 21 - object at any time to the processing of personal data
- Article 22 - not be subject to not automatic data processing and profiling

Not complying with the above articles means a data subject can go after compensation through engaging with a solicitor and complaining to a court (Article 79 & Article 80). Or through a complaint to the ICO (Article 77) which has the infamous up to 20M Euro or 4% of global turnover fine potential.

Should go without saying, the security of any internet facing portal hosting personal data on mass, needs to be highly robust and security tested via penetration testing at least annually and after any significant change.

The Information Security Breach GDPR Fines Truth

A breach of Information Security means an up to 10 Million Euro (not 20 Million Euro) or up to 2% of global turnover (not 4%)

Article 83 states *"be subject to administrative fines up to 10,000,000 EUR, or in the case of an undertaking, up to 2 % of the total worldwide annual turnover of the preceding financial year, whichever is higher: - (a) the obligations of the controller and the processor pursuant to Articles 8, 11,* ***25 to 39*** *and 42 and 43"* - Articles 32, 33, & 34 are the information security requirements, the higher level penalty rates are for privacy breaches.

The GDPR Right to Data Protection (not that clear-cut)

Recital 1 is titled **"*Data Protection as a fundamental right*"**

but **Recital 4** states "***The right to the protection of data is not an absolute right*****"** and goes on to state "*it must be considered in relation to its function in society and be* ***balanced against other fundamental rights,*** *in accordance with the principle of proportionality*".

So the GDPR is rights-based and respects all other EU 'rights', which must include the right of '***the freedom to conduct business***' as stipulated in various EU Charters and Treaties, remember the EU is founded upon a free trading block of countries not as a nation state. I am not a lawyer so I am not making a conclusion, but pointing out what might be an area of interest to lawyers fighting GDPR enforcement penalties.