Getting there – Getting the organisation ready for GDPR

This section sets out how Il7 will help an organisation approach GDPR compliance. As IT security consultants with an emphasis on information assurance and risk management, IL7 propose to address compliance from an ICT departments perspective. This brief paper gives advice on the steps organisations have to take now and demonstrates IL7's awareness and ability to help.

Already on this site is a paper saying how working towards, indeed achieving ISO/IEC 27001:2013 will help. But it will not go the whole distance. Achieving Cyber Essentials (or CE+) will also take you close. While CE addresses configuration and derives an excellent security posture, ISO 27001 will provide organisational governance as well as policies and procedures based on best practice for when business is going good – it will also ensure processes are in place for when things go wrong. But neither ISO 27001 or CE+ are enough. For GDPR we need to develop the full picture. If you are not collecting, storing, processing or transferring Personally Identifiable Information then the regulation need not apply. But if you are, and importantly if you are using data analytics and profiling personal data, the regulation applies and goes further than the DPA 1998.

In the first instance, conduct a risk assessment of the business – does it have to comply? What will happen if it doesn't? When does it need to comply? Briefly catalogue the main systems and third part relationships and ask what sort of personal data is processed?

- Identification data (name, telephone, email address (if provided on HR data or through investigation by the supplier)), possible location data, usage data (including interaction with other users). Yes/No
- Transaction data (purchases, transaction amount, etc.): Potentially through cost based services such as charity donations, traffic updates etc.
- Financial data (bank account, credit card details, etc.): Yes/No
- Location data: Landline location from telephony and potentially GPS data from mobile. Also secondary information through usage (e.g. text message from abroad): Yes/No
- Technical/Device data (IP or MAC address): IMEI data from mobiles, switch data from routers, possible IP addresses. Yes/No
- Sensitive data (as listed earlier): Yes/No.
- Criminal data (convictions, offences, etc.): Yes/No
- Other types of data: Calls made using Government telephony assets, hardware data. Yes/No
- Biometric Data Yes/No
- Identifiable/attributable metadata or cookies? Yes/No

From this exercise the organisation can qualify where it is with regards to GDPR. It must now take the following steps to quantify and address what needs to be done. As with ISO/IEC 27001:2013, a project should be initiated but without further investigation, the resources required, timeframe and outcomes cannot be quantified.

Step 1 Create a GDPR Governance Framework

Get management buy-in. Tell them about the potential penalties but talk also about the risk and consequences to operations, finance and reputation if there is a reported breach. Ensure the board appoints a Data Protection Officer, the actual or delegate from the senior Information Asset Owner (IAO), CSIO or SIRO. Ensure all other stakeholders (Data Controllers, Data Processors, internal or external IAOs) know – a good way of informing all staff is to create a portal on the organisation intranet.

Step 2 – Data Landscaping. This is a more formal exercise than the preliminary risk assessment (see above) but in this case the main systems should be examined, analysed in terms not of organisational risk (Reputation, Compliance, Operations, Finance) but of the privacy risks to the individual. They must also be examined in terms of the ability to satisfy the data subjects rights as a citizen – to access, examine, change, have deleted information as well as portability. Checks need to be made on whether all processing/profiling is necessary, is legal, has consent and if not can it be deleted without affecting other regulatory and contractual obligations. It should be recognised that industries such as law, banking, gambling and many others are regulated and this often determines the ability or not to delete data. Similarly, HMG, Police Forces and Defence have other obligations that prevent disclosure, erasure and the like. There are a number of necessary stages to data landscaping that need to tackled and the GDPR need to engage SMEs to complete these.

1. ENGAGE – Get buy in from ICT administrators and managers, set out a schedule so all are aware of what is needed.
2. ANALYSE – track information input (from customer/supplier/citizen etc) through the system processes – where (what) data is entered, what might be inferred (profiling), what is created or derived, what is passed on (to whom, or what system), when and why. Ask ‘why’ lots of time and record the answers. Have the SME draw a data flow diagram including protocols, interfaces and any encryption used. This is often referred to as SIPOC (Source-Input-Process-Output-Customer).
3. CLASSIFY – assign values to the impact of compromise – health or finance data *might* be more sensitive than hair colour, favourite chocolate etc. Take into account the media being used (video, photos, recordings etc.). Remember GDPR covers Confidentiality, Integrity and Availability – it is not just the privacy of sensitive data.
4. DISCOVER – Organise data types by classification. Map how data is stored, accessed and shared. Is it published, sold on, backed up in the cloud – where? Develop and document a chain of responsibilities.
5. ORGANISE – Plan to migrate from old systems that can’t be adjusted to comply. Provide solutions to those that can be adjusted. Implement encryption, pseudonymising or anonymising as appropriate or introducing

procedures and security enforcing functionality where needed. Document findings and proposals and document reasons why in the event that things can't in the short-term be changed and agree strategy and justification with the DPO so if there is a data subject request that can't be met, or in the event of a breach this needs to be explained, make sure it can be. One of the core outcomes of GDPR is transparency.

6. Implement a process to 'accredit' all new systems, all planned changes to systems for GDPR compliance. Develop a template for a Data Protection Impact Assessment to be completed by all projects. The template should be section into:
    a. Introduction and Project Description.
    b. Information Asset Identification (data types and classification)
    c. Data Flows and mapping (se SIPOC above).
    d. Lawfulness of Processing including contractual and regulatory considerations.
    e. Data Privacy Assessment.
    f. Integral ability to satisfy data subject requests.
    g. Integral Controls (Privacy, Cookie Policy, Access Control, encryption, pseudonymising or anonymising, Security Enforcing functions.
    h. Accreditation Findings (to be input by DPO).
    i. Additional privacy controls required (to be input by DPO).
    j. Status of additional controls and security case for 'licence to operate' (project)
    k. Recommendations (DPO)
    l. Sign Off – CISO/SIRO etc.
7. Educate all staff in the new processes and procedures and the ethics of privacy and transparency.
8. Audit and Enforce – demonstrate commitment by having a GDPR compliance programme with an annual internal audit (similar to ISO 27001).