Network and Information Systems Directive

1 Executive Summary

A European initiative to secure essential infrastructure, it was introduced alongside GDPR and covers many of the security requirements that would represent good practice. It sets out a number of Principles that should be followed. It is managed by the NCSC, but they have no governance role. This document will primarily inform and assist those responsible for technical implementation, but would also benefit those with executive responsibility through an overview understanding of the subject headings. Much of the content is taken from the NCSC or ICO website, and links are left in for further study of any of the identified fields on those sites. Most organisations will already be compliant with the points under 4A, but it is likely that we will all be continuously improving aspects from B4 onwards.

2 NCSC Extract as follows – Explains the Principles based approach

While recognising the risk of over-simplifying a complex subject, there are two basic approaches available when aiming to drive change towards a recognised desirable end-state.

The first approach is to create a set of prescriptive rules that, if closely followed, will result in achieving the desirable end-state.

The second approach is to define a set of principles that, if consistently used to guide decision-making, will collectively result in the desirable end-state.

Much has been written about the advantages and disadvantages of the two approaches, but it is the NCSC view that the principles-based approach is more effective as a way of driving improvements to cyber security in the context of the NIS Directive.

To work well, a set of prescriptive rules needs to cater for all eventualities. When this is possible, and the rules are followed, the approach can deliver what is required. However, in complex topic areas and rapidly changing circumstances, it may be impossible to cater for all eventualities.

In such cases, which include cyber security, all attempts to devise and apply a set of prescriptive rules is almost certain to lead to unintended consequences, resources being badly misallocated, and limited benefit.

While it is not possible to devise an effective set of prescriptive rules for good cyber security, it is possible to state a set of principles as a guide to cyber security decision-making. NCSC has developed such a set of principles for the implementation of the NIS Directive.

3 Implementation

- Understand the principles and why they are important. Interpret the principles for the organisation.
- Compare the outcomes described in the principles to the organisation's current practices. Use the guidance to inform the comparison.
- Identify shortcomings. Understand the seriousness of shortcomings using organisational context and prioritise.
- Implement prioritised remediation. Use the guidance to inform remediation activities.

4 The following Principles taken from the ICO

Outcomes

A) Manage security risk
You have appropriate organisational structures, policies, and processes in place to understand, assess and systematically manage security risks to personal data

A.1 Governance

You have appropriate data protection and information security policies and processes in place. If required, you ensure that you maintain records of processing activities, and have appointed a Data Protection Officer.

A.2 Risk management

You take appropriate steps to identify, assess and understand security risks to personal data and the systems that process this data.
GDPR emphasises a risk-based approach to data protection and the security of your processing systems and services. You must take steps to assess these risks and include appropriate organisational measures to make effective risk-based decisions based upon:

- the state of the art [of technology]
- cost of implementation
- the nature, scope, context and purpose of processing', and
- the severity and likelihood of the risk being realised.

Beyond this, where the processing is likely to result in a high risk to the rights and freedoms of individuals, you must also undertake a Data Protection Impact Assessment (DPIA) to determine the impact of the intended processing on the protection of personal data. The DPIA should consider the technical and organisational measures necessary to mitigate that risk. Where such measures do not reduce the risk to an acceptable level, you need to have a process in place to consult with the ICO before you start the processing.

A.3 Asset management

You understand and catalogue the personal data you process and can describe the purpose for processing it. You also understand the risks posed to individuals of any unauthorised or unlawful processing, accidental loss, destruction or damage to that data.

The personal data you process should be adequate, relevant and limited to what is necessary for the purpose of the processing, and it should not be kept for longer than is necessary.

A.4 Data processors and the supply chain

You understand and manage security risks to your processing operations that may arise as a result of dependencies on third parties such as data processors. This includes ensuring that they employ appropriate security measures.

In the case of data processors, you are required to choose those that provide sufficient guarantees about their technical and organisational measures. The GDPR includes provisions where processors are used, including specific stipulations that must feature in your contract.

B) Protect personal data against cyber attack

You have proportionate security measures in place to protect against cyber attack which cover:

- the personal data you process and
- the systems that process such data

B.1 Service Protection Policies and Processes

You should define, implement, communicate and enforce appropriate policies and processes that direct your overall approach to securing systems involved in the processing of personal data.

You should also consider assessing your systems and implementing specific technical controls as laid out in appropriate frameworks (such as Cyber Essentials).

B.2 Identity & Access Control

You understand, document and manage access to personal data and systems that process this data. Access rights granted to specific users must be understood, limited to those users who reasonably need such access to perform their function and removed when no longer needed. You should undertake activities to check or validate that the technical system permissions are consistent with your documented user access rights.

You should appropriately authenticate and authorise users (or automated functions) that can access personal data. You should strongly authenticate users who have privileged access and consider two-factor or hardware authentication measures.

You should prevent users from downloading, transferring, altering or deleting personal data where there is no legitimate organisational reason to do so. You should appropriately constrain legitimate access ensure there is an appropriate audit trail.

You should have a robust password policy which avoids users having weak passwords, such as those trivially guessable. You should change all default passwords remove or suspend unused accounts.

B.3 Data Security

You implement technical controls (such as appropriate encryption) to prevent unauthorised or unlawful processing of personal data, whether through unauthorised access to user devices or storage media, backups, interception of data in transit or at rest or accessing data that might remain in memory when technology is sent for repair or disposal.

B.4 System Security

You implement appropriate technical and organisational measures to protect systems, technologies and digital services that process personal data from cyber attack.

Whilst the GDPR requires a risk-based approach, typical expected examples of security measures you could take include:

- Tracking and recording of all assets that process personal data, including end user devices and removable media.
- Minimising the opportunity for attack by configuring technology appropriately, minimising available services and controlling connectivity.
- Actively managing software vulnerabilities, including using in-support software and the application of software update policies (patching) and taking other mitigating steps, where patches can’t be applied.
- Managing end user devices (laptops and smartphones etc) so that you can apply organisational controls over software or applications that interact with or access personal data.
- Encrypting personal data at rest on devices (laptops, smartphones, and removable media) that are not subject to strong physical controls.
- Encrypting personal data when transmitted electronically.
- Ensuring that web services are protected from common security vulnerabilities such as SQL injection and others described in widely-used publications such as the OWASP Top 10.
- Ensuring your processing environment remains secure throughout its lifecycle.

You also undertake regular testing to evaluate the effectiveness of your security measures, including virus and malware scanning, vulnerability scanning and penetration testing as appropriate. You record the results of any testing and remediating action plans.

Whatever security measures are put in place, whether these are your own or whether you use a third party service such as a cloud provider, you remain responsible both for the processing itself, and also in respect of any devices you operate.

B.5 Staff awareness & training

You give staff appropriate support to help them manage personal data securely, including the technology they use. This includes relevant training and awareness as well as provision of the tools they need to effectively undertake their duties in ways that support the security of personal data.

Staff should be provided with support to ensure that they do not inadvertently process personal data (eg by sending it to the incorrect recipient).

C) Detect security events

You can detect security events that affect the systems that process personal data and you monitor authorised user access to that data

C.1 Security monitoring

You appropriately monitor the status of systems processing personal data and monitor user access to that data, including anomalous user activity.

You record user access to personal data. Where unexpected events or indications of a personal data breach are detected, you have processes in place to act upon those events as necessary in an appropriate timeframe.

D) Minimise the impact

You can:

- minimise the impact of a personal data breach
- restore your systems and services
- manage the incident appropriately
- learn lessons for the future

D.1 Response and recovery planning

You have well-defined and tested incident management processes in place in case of personal data breaches. You have mitigation processes are in place that are designed to contain or limit the range of personal data that could be compromised following a personal data breach.

Where the loss of availability of personal data could cause harm, you have measures in place to ensure appropriate recovery. This should include maintaining (and securing) appropriate backups.

D.2 Improvements:

When a personal data breach occurs, you take steps to:

- understand the root cause
- report the breach to the Information Commissioner and, where appropriate, affected individuals (Satswana - via your DPO)
- Where appropriate (or required), report other relevant bodies (for example, other regulators, the NCSC and/or law enforcement) and

- take appropriate remediating action.

5 Conclusion

This is yet another useful guide to use as a check list in confirming that appropriate actions have been taken towards “privacy by design and default”.