****

**GDPR Competence**

**Development Procedure**

**Contents**

[1 Introduction 7](#_Toc484514533)

[2 Competence Development Procedure 8](#_Toc484514534)

[2.1 Assess Competence Requirements by Role 8](#_Toc484514535)

[2.2 Assess Existing Competence Levels 9](#_Toc484514536)

[2.3 Establish Competence Development Actions 10](#_Toc484514537)

[2.4 Evaluate Effectiveness 12](#_Toc484514538)

[3 Appendix A: Required Competences by Role 13](#_Toc484514539)

[3.1 Information Security Steering Group 13](#_Toc484514540)

[3.2 Information Security Manager 13](#_Toc484514541)

[3.3 Information Security Administrator 14](#_Toc484514542)

[3.4 Information Asset Owner 15](#_Toc484514543)

[3.5 Information Security Auditor 15](#_Toc484514544)

[3.6 Data Protection Officer 15](#_Toc484514545)

[3.7 Customer Information Security Administrator 16](#_Toc484514546)

**List of Tables**

[Table 1 - Competence level definitions 9](#_Toc484514547)

[Table 2 – Identifying development actions 11](#_Toc484514548)

# Introduction

In order to protect the personal data collected, stored and processed by the organization it is essential that employees and other interested parties involved in the provision of effective information security have the required competences. The consequences of not having sufficient skills available may lead to resourcing issues, failure to comply with legal requirements and increased risk to the business e.g. in the introduction of viruses.

[Organization Name] places emphasis on the provision of training to meet the needs of the business and to develop employees so that they can better fulfil their roles. Within technical departments such as IT there is a need to ensure that specific technology skills are developed and maintained within the team, particularly as these can change rapidly as technology develops, for example with new releases of software, or as new systems and controls are introduced.

The purpose of this competence development procedure is to identify whether there are currently sufficient information security-related competences available in the right areas within the organization and what skills may be required in the near future to cope with known changes affecting [Organization Name].

In order to do this, the required levels of competence for each GDPR and information security role must be identified and then compared with an understanding of the existing levels of competence of those people fulfilling the roles to produce recommendations for further competence development.

This procedure should be read in conjunction with the following documents which give more detail about the context, scope, objectives, resourcing and roles, responsibilities and authorities related to GDPR compliance: (check the Full GDPR Compliance course)

* Privacy and Personal Data Protection Policy
* Data Protection Impact Assessment Process
* GDPR Roles Responsibilities and Authorities
* Information Security Incident Response Procedure

# Competence Development Procedure

The steps involved in developing appropriate competences are described in this section.

## Assess Competence Requirements by Role

The various roles and duties required to manage and improve compliance to the GDPR are described in the document GDPR Roles, Responsibilities and Authorities and these are allocated to one or more specific individuals within the organization. In many cases, an allocated role forms part of a larger, more general role that the individual fulfils i.e. the individual’s time is not dedicated purely to information security.

The following GDPR and information security-related roles are specified:

* Information Security Steering Group
* Information Security Manager
* Information Security Administrator
* Information Asset Owner
* Information Security Auditor
* Data Protection Officer
* Customer Information Security Administrator

In order to fulfil the responsibilities of a role, an individual needs to possess a number of key competences at an appropriate level. Appendix A of this procedure gives an initial starting point for the list of key competences required by each role. This list must be updated each time this procedure is used to reflect changes to the competences needed due to technology, organizational or other reasons. It is recommended that this is done in close consultation with managers and the individuals themselves so that all relevant competences are included.

In addition to identifying the competences themselves, an agreement must be reached for the level of the competence that is required. This should be done with reference to the competence level definitions shown in Table 1 below. Again, this should be done in consultation with appropriate advisors.

Consideration should be given to the existing and known future requirements of GDPR compliance e.g. if a specific software tool is in the process of being implemented, competence in it should be included in the relevant list under the appropriate role.

The output of this procedure step is a list of roles with their required competences and levels of competence.

## Assess Existing Competence Levels

In order to assess the current competence levels of individuals that are to fulfil specific legislative and information security-related roles, a questionnaire approach is used. The people that are to take each role are first identified.

An appropriate questionnaire is then created for each role that includes all of the competences that have been identified as being required for that role. The required levels of competence should not be included within the questionnaire. All relevant staff are then asked to complete the questionnaire as objectively as possible using the competence level definitions shown in the table below.

|  |  |  |
| --- | --- | --- |
| **Skill Level** | **Summary** | **Guidance** |
| 0 | None | You have no knowledge or experience in this area and it is not part of your role. |
| 1 | Low | The competence area is used infrequently and is largely based upon observation of how others do it, with little understanding of why specific tasks are performed. Perhaps the competence area has only been practised for a relatively short period of time and is not seen as part of the individual’s job role. No formal training has been given. A general awareness. |
| 2 | Medium | The competence area is regularly practiced as part of the job role and this has probably been the case for a long enough period for the individual to feel comfortable doing it (more than a year). Informal and in some cases formal training may have been received and there is an understanding of the principles behind the skill. The individual feels competent in this area. |
| 3 | High | The competence area is seen as a particular strength and is backed by significant training, qualifications and experience over a lengthy period of time (probably more than 3 years). The principles are fully understood and the individual keeps up to date with developments in this area. They may have trained others and been responsible for developing processes and procedures and been involved in several projects which have made use of the skill. |
| 4 | Expert | The individual is externally recognised as a subject matter expert who contributes to developments in this area and may be involved in industry events such as presenting at conferences and seminars. He/she is held in high esteem by suppliers and customers and may assist in developing and testing new products and services. |

Table 1 - Competence level definitions

Individuals’ responses should then be validated by another party, depending on the nature of the individual’s role. This may be the individual’s manager or supervisor or in appropriate cases a peer review method may be used. This should ensure an increased level of consistency in the responses, as some people are more likely to over- or under-estimate their competency levels than others. Where there is disagreement about a level of competence, the situation should be discussed with the relevant individual to understand the reason for the discrepancy. If there is continued disagreement, a decision should be taken by management about which level should be used.

## Establish Competence Development Actions

Once a clear picture of required and current competences has been established for an individual within a role, the differences can be reviewed in order to identify the need for development actions. This may be done using a method as shown in Table 2 below.

In recommending development actions, one or more of the following alternatives may be considered:

* Informal training by existing staff with a higher level of competence e.g. mentoring
* Formal training via online or classroom courses
* Recruitment of additional staff with the relevant competence(s)
* Use of third party resources on an ad-hoc basis e.g. contractors or consultancy
* Use of third party resources via an agreed support contract which gives guaranteed access to the required level of competence

The choice of approach may depend on a number of factors, including available internal resources, budget and timescales.

In some circumstances it may be decided not to take action to address a perceived shortfall in competence e.g. if the requirement is likely to reduce or disappear in the near future due to known changes. The risks associated with doing this should be clearly stated.

Development actions and risks that are recommended for acceptance are then put forward to management for approval.

Name:

Role:

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Competence** | **Required**  **Level** | **Actual**  **Level** | **Difference** | **Recommended Development Action** | **Priority** |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

Table 2 – Identifying development actions

## Evaluate Effectiveness

The approved actions identified to develop competence in specific individuals should be reviewed for effectiveness both as part of employee performance reviews and regular management reviews of GDPR compliance.

Once a development action has been completed, a re-assessment should be carried out to check that it has resulted in the individual possessing the required level of competence. If this is not the case, the reasons for this should be established and, if necessary, further actions identified to achieve the required result.

Appropriate documented evidence should be retained of all actions carried out. This may include training records, mentoring logs or third party contracts.

# Appendix A: Required Competences by Role

[Note: The following competences by role will need to be tailored to your organization, including adding specific technical competences for your environment]

The following lists are intended to act as a starting point for the competences required for each of the roles related to GDPR compliance.

## Information Security Steering Group

|  |  |
| --- | --- |
| Competence | Required Level |
| GDPR legislation, interpretation and case law | 3 |
| Information security concepts, planning and control | 3 |
| Information security risk management | 3 |
| Information security policies | 3 |
| Conduct of management reviews | 3 |
| Auditing principles | 2 |
| Continual improvement | 2 |
| Information security incident management | 2 |
|  |  |

## Information Security Manager

|  |  |
| --- | --- |
| Competence | Required Level |
| GDPR legislation, interpretation and case law | 3 |
| Information security concepts, planning and control | 3 |
| Information security risk management | 3 |
| Conduct of management reviews | 3 |
| Auditing principles | 2 |
| Continual improvement | 3 |
| Principles of information security controls | 3 |
| Information security monitoring and reporting | 3 |
| Resource management | 2 |
| Information security policies | 3 |
| Organization of information security | 3 |
| Human resource security | 3 |
| Asset management | 3 |
| Access control | 3 |
| Cryptography | 3 |
| Physical and environmental security | 3 |
| Operations security | 3 |
| Communications security | 3 |
| System acquisition, development and maintenance | 3 |
| Supplier relationships | 3 |
| Information security incident management | 3 |
| Information security aspects of business continuity management | 3 |
| Compliance | 3 |
|  |  |

## Information Security Administrator

|  |  |
| --- | --- |
| Competence | Required Level |
| Information security concepts | 2 |
| Information security incident management | 2 |
| Principles of information security controls | 2 |
| Mobile device management | 3 |
| Information classification | 3 |
| Media handling | 3 |
| User access management | 3 |
| Cryptographic key management | 3 |
| Information backup | 3 |
| Event logging | 3 |
| Software installation | 3 |
| Technical vulnerability management | 3 |
| Information transfer procedures | 3 |
|  |  |

## Information Asset Owner

|  |  |
| --- | --- |
| Competence | Required Level |
| Information security concepts, planning and control | 2 |
| Information security risk management | 3 |
| Data protection impact assessments | 2 |
| Asset management | 3 |
| Principles of information security controls | 2 |
|  |  |

## Information Security Auditor

|  |  |
| --- | --- |
| Competence | Required Level |
| GDPR legislation, interpretation and case law | 3 |
| Information security concepts, planning and control | 3 |
| Planning, establishing, implementing and maintaining an audit programme | 3 |
| Auditing principles | 3 |
| Information security risk management | 3 |
| Principles of information security controls | 3 |
|  |  |

## Data Protection Officer

|  |  |
| --- | --- |
| Competence | Required Level |
| GDPR legislation, interpretation and case law | 3 |
| Information security concepts, planning and control | 2 |
| Data protection and related legislation | 3 |
| Data protection impact assessments | 3 |
| Information security risk management | 3 |
| Principles of information security controls | 3 |
|  |  |

## Customer Information Security Administrator

|  |  |
| --- | --- |
| Competence | Required Level |
| Information security concepts | 2 |
| Information security incident management | 2 |
| Principles of information security controls | 2 |
| User registration and deregistration | 3 |
| Multi-factor authentication | 3 |
| Log management | 3 |
| Capacity monitoring | 3 |
| Vulnerability scanning | 3 |
| Software operation e.g. IDS, IPS, malware protection, firewalls | 3 |
| System and network hardening | 3 |
| Remote access | 3 |
| Cryptographic key management | 3 |
| Backup and recovery, including testing | 3 |
| Clock synchronization | 3 |
| Installation and configuration of virtual servers | 3 |
| Testing and implementing security patches | 3 |
| Virtual network configuration | 3 |
|  |  |