

Data Protection European Union Security Standard

Data Protection European Union Security Standard

Published 16 May 2009

Copyright © 2001, 2002, 2003, 2009 Frank O'Dwyer

This document specifies technical and non-technical security policy for the European Union Data Protection Directive as implemented by the UK Data Protection Act 1998.

This standard contains 22 baseline controls, and 1 above baseline controls, for a total of 23 controls.

Important

All of these Security Standards and Security Policies are copyrighted. THEY ARE NOT IN THE PUBLIC DOMAIN. They are however distributed under a liberal open-source license, see Publishing these Security Standards and Policies.

Table of Contents

1. Introduction	1
1.1. Objectives	1
1.2. Scope	1
1.3. Not In Scope	1
1.4. Giving Feedback	1
1.5. Publishing these Security Standards and Policies	1
1.6. Related Documents	2
1.6.1. Generic Security Standards	2
1.6.2. Operating System Security Standards	2
1.6.3. Database Security Standards	3
1.7. Definitions	3
2. Security Compliance	4
2.1. Security Management	4
2.1.1. Ensure that all new uses of personal data by an application are made known to the data protection officer and notified to the data subjects	4
2.1.2. Ensure that all uses of personal data by a new application are made known to the data protection officer	4
2.1.3. Ensure that explicit consent is given by the data subjects for processing of sensitive personal data originally obtained for a different purpose.	5
2.1.4. Ensure you have appointed a data protection officer to manage compliance with data protection legislation.	6
3. Auditing and Monitoring	7
3.1. Events to be audited	7
3.1.1. Personal data must be kept only as long as required for the purposes for which it is to be processed.	7
3.1.2. Ensure that the application has an audit trail that captures all uses made of personal data	7
4. Other	9
4.1. Ensure that the data gathering methods employed by the application, such as forms, only gathers correct and relevant information when processing personal data.	9
4.1.1. Standard	9
4.1.2. Detailed Steps	9
4.1.3. Risks Addressed	9
4.2. Outbound recipients of personal data must be identifiable within the application	10
4.2.1. Standard	10
4.2.2. Detailed Steps	10
4.2.3. Risks Addressed	10
4.3. Cross border data transfers must be between states with equivalent data protection legislation	10
4.3.1. Standard	10
4.3.2. Detailed Steps	11
4.3.3. Risks Addressed	11
4.4. Processing must be adequate, relevant and not excessive	11
4.4.1. Standard	11
4.4.2. Detailed Steps	11
4.4.3. Risks Addressed	12
4.5. Ensure that the data subjects are notified of the purposes for which the personal data has been acquired or collected	12
4.5.1. Standard	12
4.5.2. Detailed Steps	12
4.5.3. Risks Addressed	12
4.6. Ensure that the data gathering forms include a checkbox to indicate consent received from the data subject	12

4.6.1. Standard	13
4.6.2. Detailed Steps	13
4.6.3. Risks Addressed	13
4.7. Ensure that the application only processes the minimum amount of personal data necessary to achieve the business objectives of the application.	13
4.7.1. Standard	13
4.7.2. Detailed Steps	13
4.7.3. Risks Addressed	14
4.8. All abbreviations used within the application must be viewable and reportable in an intelligible form	14
4.8.1. Standard	14
4.8.2. Detailed Steps	14
4.8.3. Risks Addressed	14
4.9. Ensure that all sources of personal data are identifiable within the application.	15
4.9.1. Standard	15
4.9.2. Detailed Steps	15
4.9.3. Risks Addressed	15
4.10. Ensure that personal data is subject to appropriate technical protection measures ...	15
4.10.1. Standard	15
4.10.2. Detailed Steps	16
4.10.3. Risks Addressed	16
4.11. Train employees to work within and understand their obligations under the Data Protection Act	16
4.11.1. Standard	16
4.11.2. Detailed Steps	16
4.11.3. Risks Addressed	17
4.12. Personal data must be protected against unlawful processing	17
4.12.1. Standard	17
4.12.2. Detailed Steps	17
4.12.3. Risks Addressed	17
4.13. The application design and documentation must include a clear description of the purposes for which personal data is being processed.	18
4.13.1. Standard	18
4.13.2. Detailed Steps	18
4.13.3. Risks Addressed	18
4.14. Personal data processed by an application must be subject to periodic maintenance	18
4.14.1. Standard	19
4.14.2. Detailed Steps	19
4.14.3. Risks Addressed	19
4.15. Ensure that the application design both now and in future phases will result in processing of personal data that is both fair and lawful.	19
4.15.1. Standard	20
4.15.2. Detailed Steps	20
4.15.3. Risks Addressed	20
4.16. Processing must be fair and lawful	20
4.16.1. Standard	20
4.16.2. Detailed Steps	20
4.16.3. Risks Addressed	21
4.17. Ensure that every category or type of personal data that your organisation processes is registered with the Data Protection registrar	21
4.17.1. Standard	21
4.17.2. Detailed Steps	21
4.17.3. Risks Addressed	22
5. Checklist	23

Chapter 1. Introduction

1.1. Objectives

The objectives of this document are:

- To provide guidance to administrators, developers, security personnel and data protection officers in implementing the UK Data Protection Act 1998.

1.2. Scope

Controls specified in this document apply to all organisations who process personal data relating to citizens of the member states of the European Union.

All of the organisation's information systems that process personal data will be subject to the policies specified within this security standard. The policies will be applied to both new and existing installations and should also be applied to organised manual systems.

1.3. Not In Scope

Compliance with this standard will not provide “in depth” security architecture or intelligent security design guidance to projects. As a consequence, for high impact or safety-critical business applications, additional guidance will still need to be sought from the Information Security team consultancy function. This standard is not a substitute for legal advice or a data protection officer.

Compliance with this standard does not negate the need for an overall security review of a proposed application. Contact the Information Security team if you are in doubt.

1.4. Giving Feedback

Your feedback to improve this document is welcome. Please let me know of your experiences in applying the controls and guidance in this standard. Are the controls effective, easy to implement, too onerous, clear, unclear, something missing? Does an exceptional case need to be covered? Let me know. Please send your comments to frankodwyer AT netscape.net. Your comments will be used to produce better free security standards for the IT community.

I also request that you give feedback where you think the controls and guidance is correct. This will let us gauge whether or not specific controls are controversial or broadly acceptable to the community, and will help us to resolve cases where we have conflicting feedback on particular content.

1.5. Publishing these Security Standards and Policies

This document may be reproduced and distributed in whole or in part, free of charge, subject to the following conditions:

- All copyright and trademark notices, and this permission notice must be preserved complete on all complete or partial copies.

- Any translation or derivative work of this document must be approved by Frank O'Dwyer in writing before distribution.
- If you distribute this guide in part, instructions for obtaining the complete version of this manual must be included, and a means for obtaining a complete version provided.
- Small portions may be reproduced as illustrations for reviews or quotes in other works without this permission notice if proper citation is given.
- Neither Frank O'Dwyer's name nor the names of any contributors may be used to endorse or promote products derived from this document without specific prior written permission.

THIS DOCUMENT IS PROVIDED BY FRANK O'DWYER AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL FRANK O'DWYER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

I would like to be informed of any plans to publish or distribute these documents, just so I know how they're being used and where they are becoming available. If you are publishing or distributing or planning to publish or distribute any of these documents, please send mail to frankodwyer AT netscape.net

1.6. Related Documents

This document should be read and applied in conjunction with the technology specific security standards that are available from the frankodwyer.com web site. Please note that some of the documents below are currently under development and as such may not as yet be available. Check back frequently for updates to this document and those documents listed below.

1.6.1. Generic Security Standards

Generic Security Standards

<http://www.frankodwyer.com/standards/index.html#generic>

Data Protection European Union Security Standard

<http://www.frankodwyer.com/standards/index.html#generic>

Application Service Provider Security Standards

<http://www.frankodwyer.com/standards/index.html#generic>

1.6.2. Operating System Security Standards

Generic Unix Security Standards

<http://www.frankodwyer.com/standards/index.html#os>

Windows NT4.0 Generic Security Standards

<http://www.frankodwyer.com/standards/index.html#os>

Windows NT4.0 Workstation Security Standards

<http://www.frankodwyer.com/standards/index.html#os>

Windows NT4.0 Server Security Standards

<http://www.frankodwyer.com/standards/index.html#os>

Windows NT4.0 Domain Security Standards

<http://www.frankodwyer.com/standards/index.html#os>

1.6.3. Database Security Standards

Oracle Security Standards

<http://www.frankodwyer.com/standards/index.html#db>

1.7. Definitions

An “Information Asset” equates to any computerised information system or component thereof and thus includes an application, an item of off the shelf software, hardware, media, a data item, a data item repository and associated communications networks.

The specification of the Information Asset in question will usually be given so that this document is unambiguous, except where a control relates to any “Information Asset”.

The use of “must” or “will” indicates what the author considers to be a mandatory control.

However, whether the controls listed here are mandatory for your organisation is entirely at your organisation's discretion and thus they should be interpreted as representing the strongest recommendation of the author.

The use of “should” or “recommended” or “ought” indicates that the author believes that the controls in question are worthwhile and should be implemented unless such an implementation is impossible, onerous or impractical. Again, the implementation of controls so recommended in this document is entirely at your organisation's discretion.

Chapter 2. Security Compliance

2.1. Security Management

2.1.1. Ensure that all new uses of personal data by an application are made known to the data protection officer and notified to the data subjects

ID	Version	Level	Enforcement
DPA-OFFICE-3	1.0	baseline	mandatory

2.1.1.1. Standard

Ensure that all new uses of personal data by an application are made known to the data protection officer and notified to the data subjects

2.1.1.2. Detailed Steps

- Identify all functional uses of personal data
- Make these known to the data protection officer
- Where appropriate notify the data subjects of the new uses

2.1.1.3. Risks Addressed

Where this control is not applied, the following residual risks exist:

- Non-compliance with legal requirements
- Censure from the Data Protection Commission
- Fines from the Data Protection Commission

2.1.2. Ensure that all uses of personal data by a new application are made known to the data protection officer

ID	Version	Level	Enforcement
DPA-OFFICE-2	1.0	baseline	mandatory

2.1.2.1. Standard

Ensure that all uses of personal data by a new application are made known to the data protection officer

2.1.2.2. Detailed Steps

- Identify all functional uses of personal data
- Make these known to the data protection officer
- Where necessary update the registration of your organisation

2.1.2.3. Risks Addressed

Where this control is not applied, the following residual risks exist:

- Non-compliance with legal requirements
- Censure from the Data Protection Commission
- Fines from the Data Protection Commission

2.1.3. Ensure that explicit consent is given by the data subjects for procesing of sensitive personal data originally obtained for a different purpose.

ID	Version	Level	Enforcement
DPA-OFFICE-4	1.0	above baseline	mandatory

2.1.3.1. Standard

Ensure that explicit consent is given by the data subjects for processing of sensitive personal data originally obtained for a different purpose.

2.1.3.2. Detailed Steps

- Identify all functional uses of sensitive personal data
- Make these known to the data protection officer
- Identify any different uses that are now being made of the personal data
- Seek explicit permission from the data subjects regarding these new uses
- Exclude those data subjects from the application database who do not provide explicit permission

2.1.3.3. Risks Addressed

Where this control is not applied, the following residual risks exist:

- Non-compliance with legal requirements
- Censure from the Data Protection Commission
- Fines from the Data Protection Commission

2.1.4. Ensure you have appointed a data protection officer to manage compliance with data protection legislation.

ID	Version	Level	Enforcement
DPA-OFFICE-1	1.0	baseline	mandatory

2.1.4.1. Standard

Ensure you have appointed a data protection officer to manage compliance with data protection legislation.

2.1.4.2. Detailed Steps

- Appoint an appropriate individual to act as the Data Protection Officer
- This may be a part time role, full time or even a team of people depending on the size of your organisation and the nature of it's activities

2.1.4.3. Risks Addressed

Where this control is not applied, the following residual risks exist:

- Non-compliance with legal requirements
- Censure from the Data Protection Commission
- Fines from the Data Protection Commission

Chapter 3. Auditing and Monitoring

3.1. Events to be audited

3.1.1. Personal data must be kept only as long as required for the purposes for which it is to be processed.

ID	Version	Level	Enforcement
DPA-APP-11	1.0	baseline	mandatory

3.1.1.1. Standard

Personal data must be kept only as long as required for the purposes for which it is to be processed.

3.1.1.2. Detailed Steps

- Identify every item of personal data to be processed
- For each data item determine a lifetime
- Ensure that the personal data is deleted at the expiry of that lifetime

3.1.1.3. Risks Addressed

Where this control is not applied, the following residual risks exist:

- Non-compliance with legal requirements
- Censure from the Data Protection Commission
- Fines from the Data Protection Commission

3.1.2. Ensure that the application has an audit trail that captures all uses made of personal data

ID	Version	Level	Enforcement
DPA-APP-10	1.0	baseline	mandatory

3.1.2.1. Standard

Ensure that the application has an audit trail that captures all uses made of personal data

3.1.2.2. Detailed Steps

- Ensure that every application function that is used to read, write, change or delete personal data fields generates and audit record.
- The audit record must contain at minimum the user id associated with the action, the date and time, the action itself and the source of the user login

3.1.2.3. Risks Addressed

Where this control is not applied, the following residual risks exist:

- Non-compliance with legal requirements
- Censure from the Data Protection Commission
- Fines from the Data Protection Commission
- Business information being subject to unauthorised disclosure
- Business information being subject to unauthorised modification
- Business information being unavailable

Chapter 4. Other

4.1. Ensure that the data gathering methods employed by the application, such as forms, only gathers correct and relevant information when processing personal data.

ID	Version	Level	Enforcement
DPA-APP-7	1.0	baseline	mandatory

4.1.1. Standard

Ensure that the data gathering methods employed by the application, such as forms, only gathers correct and relevant information when processing personal data.

4.1.2. Detailed Steps

- Ensure that only required data is collected
- Ensure that only registered processing purposes of that data is performed
- Ensure that data integrity checks are performed on the data to ensure that it is reasonable
- Ensure that the other controls in this security stanhdard are adhered to.

4.1.3. Risks Addressed

Where this control is not applied, the following residual risks exist:

- Non-compliance with legal requirements
- Censure from the Data Protection Commission
- Fines from the Data Protection Commission
- Business information may be subject to unauthorised disclosure
- Business information may be unavailable
- Business information may be subject to a loss of integrity

4.2. Outbound recipients of personal data must

be identifiable within the application

ID	Version	Level	Enforcement
DPA-APP-2	1.0	baseline	mandatory

4.2.1. Standard

Ensure that all outbound recipients of personal data from this application are identifiable in the application.

4.2.2. Detailed Steps

- Identify all of the personal data processed by the application
- For each data item to determine all of the outbound recipients of the data
- Ensure that the application logic is able to both display and report on the outbound recipients of the personal data

4.2.3. Risks Addressed

Where this control is not applied, the following residual risks exist:

- Non-compliance with legal requirements
- Censure from the Data Protection Commission
- Fines from the Data Protection Commission
- Business information may be subject to unauthorised disclosure
- Business information may be unavailable

4.3. Cross border data transfers must be between states with equivalent data protection legislation

ID	Version	Level	Enforcement
DPA-PROC-5	1.0	baseline	mandatory

4.3.1. Standard

Ensure that no personal data is transferred outside the European Union unless the destination country and any intermediate countries have adopted legislation that offers an equivalent or higher level of data protection.

4.3.2. Detailed Steps

- Identify non European Union destinations for personal data
- Determine whether their data protection legislation offers similar protection as that afforded in EU member states
- Where it does not, do not transfer the data

4.3.3. Risks Addressed

Where this control is not applied, the following residual risks exist:

- Non-compliance with legal requirements
- Censure from the Data Protection Commission
- Fines from the Data Protection Commission
- Unauthorised disclosure of business information
- Unauthorised modification of business information

4.4. Processing must be adequate, relevant and not excessive

ID	Version	Level	Enforcement
DPA-PROC-2	1.0	baseline	mandatory

4.4.1. Standard

Ensure that all personal data to be processed is adequate, relevant and not excessive in relation to the purposes for which it is processed.

4.4.2. Detailed Steps

- Collect only the personal data that you need
- Process the personal data in accordance with your organisations registered uses

4.4.3. Risks Addressed

Where this control is not applied, the following residual risks exist:

- Non-compliance with legal requirements
- Censure from the Data Protection Commission
- Fines from the Data Protection Commission

4.5. Ensure that the data subjects are notified of the purposes for which the personal data has been acquired or collected

ID	Version	Level	Enforcement
DPA-DATA-2	1.0	baseline	mandatory

4.5.1. Standard

Ensure that the data subjects are notified of the purposes for which the personal data has been acquired or collected

4.5.2. Detailed Steps

- On all collection forms include a section describing the uses that the personal data will be put to
- Periodically notify the data subjects of the uses of personal data that has been collected.

4.5.3. Risks Addressed

Where this control is not applied, the following residual risks exist:

- Non-compliance with legal requirements
- Censure from the Data Protection Commission
- Fines from the Data Protection Commission

4.6. Ensure that the data gathering forms include a checkbox to indicate consent received from the data subject

ID	Version	Level	Enforcement
DPA-APP-8	1.0	baseline	mandatory

4.6.1. Standard

Ensure that the data gathering forms include a checkbox to indicate that consent has been received from the data subject for the processing

4.6.2. Detailed Steps

- Include a consent field on the forms for the data subject to indicate whether consent has been obtained

4.6.3. Risks Addressed

Where this control is not applied, the following residual risks exist:

- Non-compliance with legal requirements
- Censure from the Data Protection Commission
- Fines from the Data Protection Commission

4.7. Ensure that the application only processes the minimum amount of personal data necessary to achieve the business objectives of the application.

ID	Version	Level	Enforcement
DPA-APP-9	1.0	baseline	mandatory

4.7.1. Standard

Ensure that the application only processes the minimum amount of personal data necessary to achieve the business objectives of the application.

4.7.2. Detailed Steps

- Verify that every field of personal data is justified in relation to the registered purposes and the pro-

cessing required.

4.7.3. Risks Addressed

Where this control is not applied, the following residual risks exist:

- Non-compliance with legal requirements
- Censure from the Data Protection Commission
- Fines from the Data Protection Commission
- Unauthorised disclosure of business information

4.8. All abbreviations used within the application must be viewable and reportable in an intelligible form

ID	Version	Level	Enforcement
DPA-APP-12	1.0	baseline	mandatory

4.8.1. Standard

Ensure that the application includes definitions for all abbreviations or codes used in the application so as to allow data subjects to have relevant information disclosed in an intelligible form.

4.8.2. Detailed Steps

- Identify all abbreviations, acronyms, codes etc
- For each one that is used ensure that when viewing or reporting data a means of eliciting the full meaning is available

4.8.3. Risks Addressed

Where this control is not applied, the following residual risks exist:

- Non-compliance with legal requirements
- Censure from the Data Protection Commission
- Fines from the Data Protection Commission

4.9. Ensure that all sources of personal data are identifiable within the application.

ID	Version	Level	Enforcement
DPA-APP-1	1.0	baseline	mandatory

4.9.1. Standard

Ensure that all sources of personal data are identifiable within the application.

4.9.2. Detailed Steps

- Ensure that all fields or files that will contain personal data are identified
- Ensure that for each data item to be stored that a source attribute is include
- Ensure that the application logic has the ability to both display and report on the sources of data
- Ensure that unknown sources of personal data are validated through a subject survey or deleted

4.9.3. Risks Addressed

Where this control is not applied, the following residual risks exist:

- Non-compliance with legal requirements
- Censure from the Data Protection Commission
- Fines from the Data Protection Commission
- Business information may be subject to a loss of integrity
- Business information may be unavailable

4.10. Ensure that personal data is subject to appropriate technical protection measures

ID	Version	Level	Enforcement
DPA-PROC-3	1.0	baseline	mandatory

4.10.1. Standard

Ensure that all the personal data is subject to appropriate technical measures to protect against unauthorised or unlawful processing and accidental loss, destruction or damage.

4.10.2. Detailed Steps

- Perform a risk analysis against all applications or systems that process personal data
- Define a technical security architecture in line with the results of the risk analysis
- Retain the risk analysis documentation and reports to provide an audit trail of the reasoning behind the technical measures deployed

4.10.3. Risks Addressed

Where this control is not applied, the following residual risks exist:

- Non-compliance with legal requirements
- Censure from the Data Protection Commission
- Fines from the Data Protection Commission
- Business information may be subject to unauthorised disclosure
- Business information may be subject to a loss of integrity
- Business information may be unavailable

4.11. Train employees to work within and understand their obligations under the Data Protection Act

ID	Version	Level	Enforcement
DPA-PROC-6	1.0	baseline	mandatory

4.11.1. Standard

Ensure that employees dealing with the personal data processed by this application have been trained so as to understand the principles of the Data Protection Act and the impact that these principles have on the way they work.

4.11.2. Detailed Steps

- Train the employees who handle/process personal data to understand the data protection act and how this impacts working practices.

4.11.3. Risks Addressed

Where this control is not applied, the following residual risks exist:

- Non-compliance with legal requirements
- Censure from the Data Protection Commission
- Fines from the Data Protection Commission
- Unauthorised disclosure of business information
- Unauthorised modification of business information
- Unauthorised loss of business information

4.12. Personal data must be protected against unlawful processing

ID	Version	Level	Enforcement
DPA-PROC-4	1.0	baseline	mandatory

4.12.1. Standard

Ensure that all the personal data is subject to appropriate organisational measures to protect against unauthorised or unlawful processing and accidental loss, destruction or damage.

4.12.2. Detailed Steps

- Ensure that access to personal data is based upon requirements of a role and is authorised by the application or business process owner

4.12.3. Risks Addressed

Where this control is not applied, the following residual risks exist:

- Non-compliance with legal requirements
- Censure from the Data Protection Commission
- Fines from the Data Protection Commission
- Unauthorised disclosure of business information
- Unauthorised modification of business information
- Loss of availability of business information

4.13. The application design and documentation must include a clear description of the purposes for which personal data is being processed.

ID	Version	Level	Enforcement
DPA-APP-5	1.0	baseline	mandatory

4.13.1. Standard

Ensure that the application design and documentation includes a clear description of the purposes for which personal data is being processed.

4.13.2. Detailed Steps

- Identify the application data to be processed
- Identify the processes that are to be performed on the personal data
- Ensure that the data and the processes to be performed are documented

4.13.3. Risks Addressed

Where this control is not applied, the following residual risks exist:

- Non-compliance with legal requirements
- Censure from the Data Protection Commission
- Fines from the Data Protection Commission
- Business information may be subject to unauthorised disclosure
- Business information may be unavailable
- Business information may be subject to a loss of integrity

4.14. Personal data processed by an application must be subject to periodic maintenance

ID	Version	Level	Enforcement
DPA-APP-4	1.0	baseline	mandatory

4.14.1. Standard

Ensure that a schedule of maintenance for the personal data that is processed by this application is developed and includes destruction and retention.

4.14.2. Detailed Steps

- Identify all of the personal data processed by the application
- Create a schedule of periodic maintenance
- Ensure the schedule includes validation
- Ensure the schedule includes destruction of data that is no longer required to be held or data that is no longer correct and does not required to be held for historical purposes
- Ensure that the schedule includes retention/archiving for personal data that must be kept for historic or regulatory reasons or otherwise for lawful processing

4.14.3. Risks Addressed

Where this control is not applied, the following residual risks exist:

- Non-compliance with legal requirements
- Censure from the Data Protection Commission
- Fines from the Data Protection Commission
- Business information may be subject to unauthorised disclosure
- Business information may be unavailable

4.15. Ensure that the application design both now and in future phases will result in processing of personal data that is both fair and lawful.

ID	Version	Level	Enforcement
DPA-APP-6	1.0	baseline	mandatory

4.15.1. Standard

Ensure that the application design both now and in future phases will result in processing of personal data that is both fair and lawful.

4.15.2. Detailed Steps

- Ensure the application design complies with the controls in this standard
- Ensure that the application design complies with the requirements of your organisations legal department and data protection office

4.15.3. Risks Addressed

Where this control is not applied, the following residual risks exist:

- Non-compliance with legal requirements
- Censure from the Data Protection Commission
- Fines from the Data Protection Commission
- Business information may be subject to unauthorised disclosure
- Business information may be unavailable
- Business information may be subject to a loss of integrity

4.16. Processing must be fair and lawful

ID	Version	Level	Enforcement
DPA-PROC-1	1.0	baseline	mandatory

4.16.1. Standard

Ensure that all personal data that is to be processed i.e. collected, organised, stored, retrieved, disclosed or destroyed is done so fairly and lawfully.

4.16.2. Detailed Steps

- Ensure categories of data collected match that which are actually collected
- Ensure that the uses of the data match the uses for which your organisation is registered.
- Ensure that data subjects are aware of the data that your organisation collects about them
- Ensure that data subjects are aware of the processing of the data that your organisation performs

- Ensure that as a minimum you comply with all of the controls in this security standard
- Ensure one of the following conditions are satisfied
 - - The data subject gives his or her consent to the processing or If the data subject is an employee or a prospective employee, ensure that the processing is necessary for the performance of a contract to which the employee is a party or for the taking of steps at the prospective employees request with a view to entering into a contract.
 - - The processing is necessary for compliance with a legal obligation.
 - - The processing is necessary to protect the interests of the data subject
 - - The processing is necessary in the public interest or in the exercise of official authority
 - - The processing is necessary for the purposes of the legitimate interests of the processing party except where these interests are overridden by the fundamental rights and freedom of the data subject.

4.16.3. Risks Addressed

Where this control is not applied, the following residual risks exist:

- Non-compliance with legal requirements
- Censure from the Data Protection Commission
- Fines from the Data Protection Commission

4.17. Ensure that every category or type of personal data that your organisation processes is registered with the Data Protection registrar

ID	Version	Level	Enforcement
DPA-DATA-1	1.0	baseline	mandatory

4.17.1. Standard

Ensure that every category or type of personal data that your organisation processes is registered with the Data Protection registrar

4.17.2. Detailed Steps

- Identify every category or type of personal data processed by your organisation
- Register these data types with the data protection registrar

- Put in place a process to ensure that this is maintained up to date
- For a new application processing personal data perform a gap analysis to determine whether new categories of personal data are to be processed
- Update your organisation's registration accordingly

4.17.3. Risks Addressed

Where this control is not applied, the following residual risks exist:

- Non-compliance with legal requirements
- Censure from the Data Protection Commission
- Fines from the Data Protection Commission

Chapter 5. Checklist

<i>Security Compliance</i>		
<i>Security Management</i>		
<i>Control ID</i>	<i>Checklist Question</i>	<i>Your Answer</i>
DPA-OF-FICE-3	Has it been ensured that all new uses of personal data by an application are made known to the data protection officer and notified to the data subjects?	
DPA-OF-FICE-2	Have you ensured that all uses of personal data by a new application have been made known to the data protection officer?	
DPA-OF-FICE-4	Has it been ensured that explicit consent has been given by the data subjects for processing of sensitive personal data originally obtained for a different purpose?	
DPA-OF-FICE-1	Have you have appointed a data protection officer to manage compliance with data protection legislation?	
<i>Auditing and Monitoring</i>		
<i>Events to be audited</i>		
<i>Control ID</i>	<i>Checklist Question</i>	<i>Your Answer</i>
DPA-APP-11	Is personal data kept only as long as required for the purposes for which it is to be processed?	
DPA-APP-10	Does the application have an audit trail that captures all uses made of the personal data?	
<i>Other</i>		
<i>Control ID</i>	<i>Checklist Question</i>	<i>Your Answer</i>
DPA-APP-7	Is it ensured that the data gathering methods employed by the application, such as forms, only gathers correct and relevant information when processing personal data?	
DPA-APP-2	is it ensured that all outbound recipients of personal data from this application are identifiable in the application?	
DPA-PROC-5	Is it ensured that no personal data is transferred outside the European Union unless the destination and intermediate countries have adopted legislation that offers an equivalent or higher level of data protection?	
DPA-PROC-2	Have you ensured that all personal data to be processed is adequate, relevant and not excessive in relation to the purposes for which it is processed?	
DPA-DATA-2	Do you ensure that the data subjects are notified of the purposes for which the personal data has been acquired or collected?	
DPA-APP-8	Is it ensure that the data gathering forms include a checkbox to indicate that consent has been received from the data subject for the processing to take place?	
DPA-APP-9	Has it been ensured that the application only processes the minimum	

Checklist

	amount of personal data necessary to achieve the business objectives of the application?	
DPA-APP-12	Has it been ensured that the application includes definitions of all abbreviations or codes used to allow data subjects to have relevant information disclosed in an intelligible form.	
DPA-APP-1	Is it ensured that all sources of personal data are identifiable within the application?	
DPA-PROC-3	Have you ensured that all personal data is subject to appropriate technical measures to protect against unauthorised or unlawful processing and accidental loss, destruction or damage.	
DPA-PROC-6	Have employees that deal with the personal data processed by this application been trained so as to understand the principles of the Data Protection Act and the impact that these principles have on the way they work?	
DPA-PROC-4	Is the personal data subject to appropriate organisational measures to protect against unauthorised or unlawful processing and accidental loss, destruction or damage?	
DPA-APP-5	Does the application design and documentation include a clear description of the purposes for which personal data is being processed?	
DPA-APP-4	Has it been ensured that a schedule of maintenance for the personal data that is processed by this application has been developed that includes destruction and retention.	
DPA-APP-6	Will the application design both now and in future phases result in processing of personal data that is both fair and lawful.	
DPA-PROC-1	Ensure that all personal data that is to be processed i.e. collected, organised, stored, retrieved, disclosed or destroyed is done so fairly and lawfully.	
DPA-DATA-1	Have you ensured that every category or type of personal data that your organisation processes is registered with the Data Protection registrar?	