Data Protection Impact Assessment

Milk Student Planner

Approved on 14/05/2017

Abstract

Milk Student Planner System is a service, provided by Milk Student Planners Limited, that facilitates secure data viewing between institutions and the staff, students, parents and care givers they authorize. This data protection impact assessment (privacy impact assessment) identifies data protection (privacy and security) risks and any legal obligations regarding the data processed by Milk Student Planner System, and the steps we at Milk Student Planners Limited have taken to ensure data is handled both ethically and legally.

Revision History

Version	Date	Contributor	Modifications
0.1	Mar 2018	Michael Dowling-Fleet	Initial version

Copyright and Commercial Statement

Copyright © Milk Student Planner Limited. All rights reserved.

This document is commercial-in-confidence. The recipient of this document agrees to hold all information presented within as confidential and agree not to use or disclose, or allow to use or disclosure of the said information to unauthorized parties, directly or indirectly, irrespective of the acceptance or rejection of the presentation or at any time before, during or after an agreement has been reached, without prior written consent.

No part of this publication may be reproduced, distributed, or transmitted in any form or by any means, including photocopying, recording, or other electronic or mechanical methods, without prior written consent, except in the case of brief quotations and other non-commercial uses permitted by copyright law.

To request consent to relaxing the above, write to Milk Student Planner Limited, 4B Church St, Diss, Norfolk, IP22 4DD, UK.

Disclaimer

This document and the information contained herein is provided on an “as is” basis and Milk Student Planner Limited disclaims all warranties, express or implied, including but not limited to any warranty that the use of the information herein will not infringe any rights or any implied warranties of merchantability or fitness for a purpose.

Table of Contents

An Introduction to Data Protection Impact Assessments

The General Data Protection Regulation (GDPR, article 35) (European Parliament, 2016) defines Data Protection Impact Assessments (DPIAs). For the purposes of data protection a PIA can be used as a DPIA.

The ICO (Information Commissioner's Office, 2014) defines Privacy Impact Assessments (PIAs) as “a process which assists organisations in identifying and minimising the privacy risks of new projects or policies.” As such they are a tool best employed early in a project’s development when addressing risks is often simpler and less costly. PIAs also help build trust in the safe handling of data through transparency and accountability.

PIAs are not static documents since data and its risks will change over time; they should evolve with their respective projects and be regularly reviewed both internally and externally. A typical PIA cycle involves:

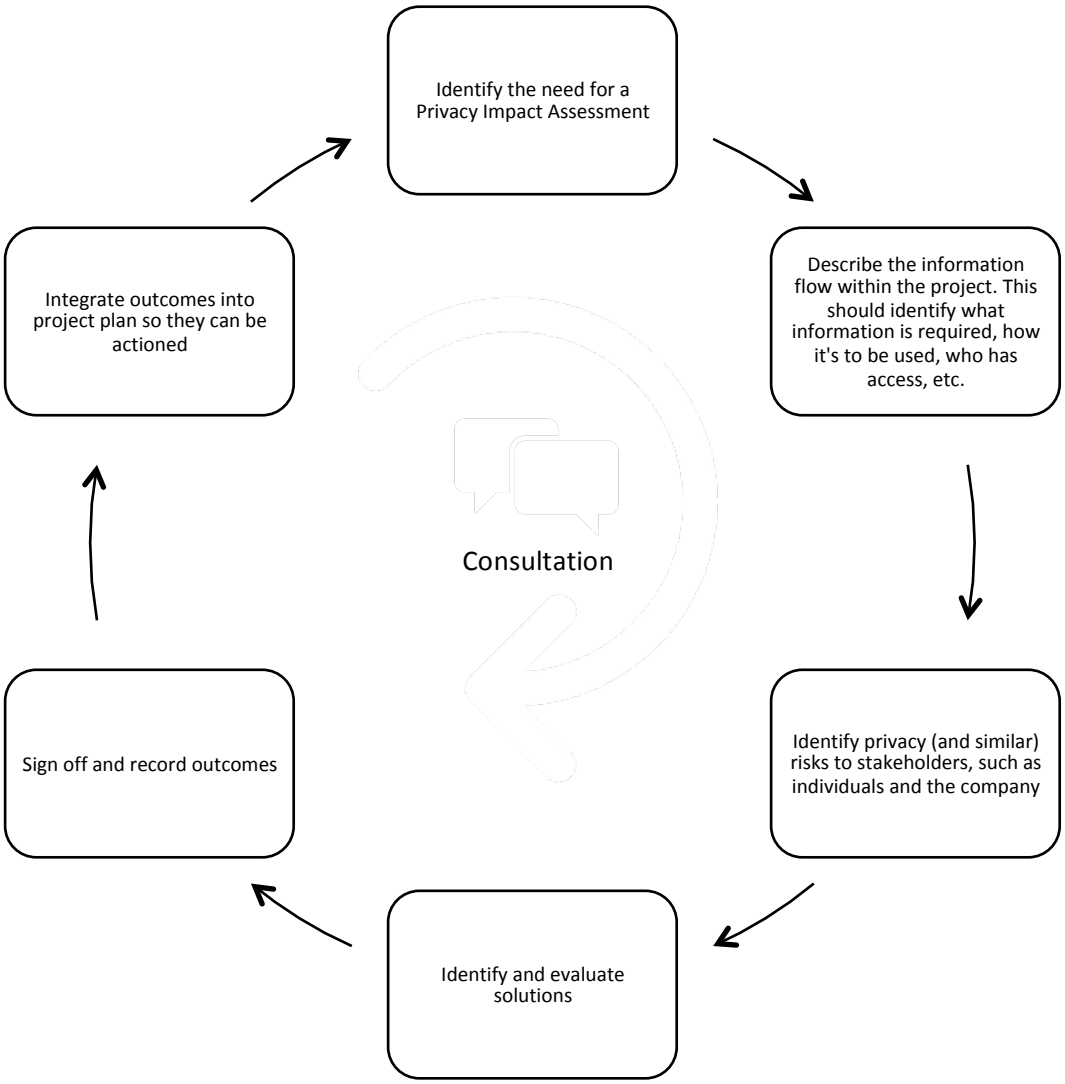

Figure 1: Stages of the Privacy Impact Assessment process

More information on Privacy Impact Assessments can be found on the Information Commissioner’s Office (Information Commissioner's Office, 2014).

It is the data controller’s responsibility to ensure they have their own data protection impact assessment in place for the transfer of data to data processors. The data controller must ensure they have legitimate interest (including consent where required) for all data to be sent to data processors.

Milk Student Planner System

URL	https://milkstudentplanner.com (https://my.milkapp.io)	
Project Owner	Michael Dowling-Fleet	Chief Executive Officer
Privacy Manager	Michael Dowling-Fleet	Chief Executive Officer

Executive Summary

Milk is an online student planner system designed to boost your child's performance at school and is accessible via a web browser or any Android or Apple mobile device. It puts you in control of your homework diary with messaging features, a data rich student achievement dashboard, homework analytics and MIS integration.
Milk automatically imports all student data from leading school MIS (e.g., Capita SIMS and Bromcom). Single-sign-on options are also available. Milk's servers are in the United Kingdom and governed under The Data Protection Act.

Description of Information and Information Flow

The Milk Student Planner System (Milk) is a Data Processor on behalf of the Data Controller (education institution), authorized by Data Sharing Agreements (DSA). Milk uses ZiNET Connect (ZiNET Data Solutions Limited) to securely obtain the data it requires from the data controller over a point-to-point connection. A connector is installed with secure access to the institution's data, which resides within the data controller's purview. This data is aggregated, presented as per the SIF specification (www.a4l.org), and made available in XML (machine readable) format. The data extracted is sent directly to Milk over encrypted transport (HTTPS).

ZiNET Data Solutions Ltd enables secure data transfer between institutions and Milk, but is not itself a data processor, as shown in the figure below.

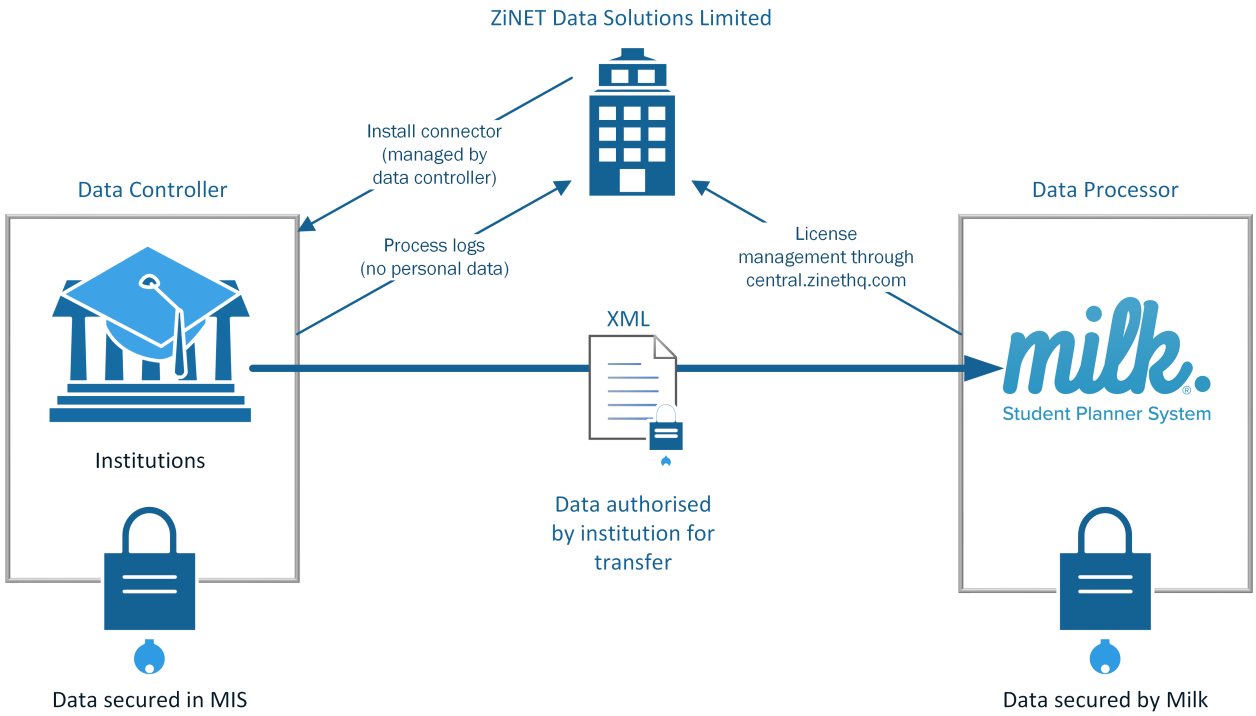

Figure 2: Information flow diagram

Data being processed

The following data will be collected from the data controller for the provision of the Milk Student Planner service:

- School information
  - Name
  - Address
  - Number of academic years
  - Subject list
  - Term dates
  - Classes and registration groups
- Student information
  - Unique Pupil Number (UPN)
  - Email address
  - Name
  - Gender
  - School year
  - Date of birth
  - Classes (and registration group)
  - Photo (optional)
  - SEN status (optional)
  - PupilPremium (optional)
  - Medical (optional)
- Staff (teacher) information
  - Name
  - Email address
  - Classes
  - Photograph (optional)
- Parent information (from MIS contacts, where available)
  - Name
  - Email address
- Timetable information on both students and staff
- Student attendance
- Student behaviour
- Student achievement points
- Student assessments & results (where available)

Rationale for data collection

Part of the core purpose of Milk is to take information that would normally only be available to staff via the establishment's Management Information System (MIS), and to make it more useful - to enable communication between staff and students, and parents, and to make information (such as attendance, where available) visible to students and their parents.

Data collected for the purpose of Milk will be used solely for that purpose and no other. For example, students and staff will never be sent marketing communications.

Data retention and update

Milk preferably syncs data from the establishment at least once per day, but this is something that can be discussed with the data controller.

All data is backed up every 24 hours, encrypted, and stored offsite within the UK (Amazon Web Services UK Ltd). Old backups are removed based on a schedule and not kept for more than 14 days.

Security of data

Before the data leaves the purview of the data controller it is filtered to the set required/agreed to be sent to Milk (ZiNET Connect).

Data is sent to Milk over secure encrypted TLS 1.2 (commonly referred to as SSL) channel.

All data is hosted in the UK.

All communications use strong TLS 1.2 encrypted and authenticated connections (commonly referred to as SSL). No non- secure access is permitted to any services.

Milk's API at rest is not encrypted at present. Some data is encrypted and some is stored in anonymity, with unique keys used for reference. The database server itself is not accessible from the public Internet. Work is ongoing to encrypt all user data in the database.

All members of the staff who have direct access to the data have

Data breaches

All parties will ensure that all other parties are promptly notified of any security breaches or significant security risks, affecting shared information.

Terminating the service

We delete any data controlled by customer upon termination of service. We require 1 working day to delete any live data and a further 1 working day to remove from our backup server.

Screening

Privacy Impact Assessment Screening

Question	Yes	No
1. Will the project involve the collection of new information about individuals?	✓	
Yes. While the majority of data viewed by the user is collected by the institution under its usual and legitimate purpose, in some cases there may be user additions to this existing data, i.e., users have the ability to enter their personal email addresses into Milk Student Planner System. Other information relevant to users collated by Milk Student Planner System is restricted to homework assignments and messages posted by teaching staff, data of which is collated for analytical use by the Data Controller. In every user case, the purpose of the data does not change beyond its normal use by the Data Controller.		
2. Will the project compel individuals to provide information about themselves?		✓
No. All data transferred is collected by the institution under their legitimate interest. Users are not compelled to supply their personal email address for the purpose of user identity verification and password resetting.		
3. Will information about individuals be disclosed to organisations or people who have not previously had routine access to the information?		✓
No. The Confidentiality clause of Milk Student Planner System's Service Level Agreement to Data Controllers states: 7.2 Neither party shall use or disclose any Confidential Information of the other party without the agreement in writing of the other party unless: (7.2.1) required to disclose such information by law; (7.2.2) or where such Confidential Information could bring into question the professionalism of an employee of the School.		
4. Are you using information about individuals for a purpose it is not currently used for, or in a way it is not currently used?		✓
No. Milk Student Planners Ltd provides software for the data controller to reformat and distribute data in a secure way. Other information relevant to users collated by Milk Student Planner System is restricted to homework assignments and messages posted by teaching staff, data of which is collated for analytical use by the Data Controller. In every user case, the purpose of the data does not change beyond its normal use by the Data Controller.		
5. Does the project involve you using new technology which might be perceived as being privacy intrusive? For example, the use of biometrics or facial recognition.		✓
No. No such technology is used by Milk Student Planner System.		
6. Will the project result in you making decisions or taking action against individuals in ways which can have a significant impact on them?		✓
No. Milk Student Planner System does not use data it collects to make decisions or take action against individuals.		
7. Is the information about individuals of a kind particularly likely to raise privacy concerns or expectations? For example, health records, criminal records or other information that people would consider to be particularly private.	✓	
Yes. Milk Student Planner System processes data related to support learning activities. This involves data such as attendance, behaviour, special educational needs, and healthcare details. This data may be considered particularly private or sensitive.		
8. Will the project require you to contact individuals in ways which they may find intrusive?		✓
No. While the Milk Student Planner System does facilitate communication with individuals, it does not require it. The Data Controller (and their authorised representatives), or other authorised users of the system contact individuals and manage their access to Milk Student Planner System.		

References

Data Protection Working Party (WP 217). (2014, April 9). *Article 29 (844/14/EN).* Retrieved July 25, 2017 from http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp217_en.pdf

Department for Education. (2016, July 1). *National database of governors.* Retrieved July 20, 2017 from https://www.gov.uk/government/news/national-database-of-governors

European Parliament. (2016, April 27). *Directive 95/46/EC (General Data Protection Regulation).* Retrieved February 15, 2017 from http://eur-lex.europa.eu/eli/reg/2016/679/oj

Information Commissioner's Office. (2014, February 25). *Conducting Privacy Impact Assessments: Code of Practice.* Retrieved February 15, 2017 from https://ico.org.uk/media/for-organisations/documents/1595/pia-code-of-practice.pdf

Information Commissioner's Office. (2017, January 31). *Guide to Data Protection.* Retrieved February 15, 2017 from https://ico.org.uk/for-organisations/guide-to-data-protection/

Information Commissioner's Office. (2017, February 10). *Overview of the General Data Protection Regulation (GDPR).* Retrieved February 15, 2017 from https://ico.org.uk/for-organisations/data-protection-reform/overview-of-the-gdpr/

Open Data Commons. (n.d.). *Open Data Commons Attribution License (ODC-By) v1.0.* Retrieved July 25, 2017 from https://opendatacommons.org/licenses/by/1.0/

Slaughter and May. (2014, May). *When is processing personal data in your legitimate interests?* Retrieved July 24, 2017 from https://www.slaughterandmay.com/media/2162779/when-is-processing-personal-data-in-your-legitimate-interests.pdf

UK Government. (1998). *Data Protection Act.* Retrieved February 14, 2017 from http://www.legislation.gov.uk/ukpga/1998/29

UK Government. (1996, July 24). *Education Act 1996.* Retrieved July 2014, 2017 from http://www.legislation.gov.uk/ukpga/1996/56

UK Government. (n.d.). *Open Government License (OGL) for Public Sector Information, version 3.* Retrieved July 25, 2017 from http://www.nationalarchives.gov.uk/doc/open-government-licence/version/3/

Appendix A: Definitions

This document uses terms as defined in (UK Government, 1998), which are presented below for reference.

data means information which—
(a) is being processed by means of equipment operating automatically in response to instructions given for that purpose,
(b) is recorded with the intention that it should be processed by means of such equipment,
(c) is recorded as part of a relevant filing system or with the intention that it should form part of a relevant filing system,
(d) does not fall within paragraph (a), (b) or (c) but forms part of an accessible record as defined by section 68; or
(e) is recorded information held by a public authority and does not fall within any of paragraphs (a) to (d);

personal data means data which relate to a living individual who can be identified—
(a) from those data, or
(b) from those data and other information which is in the possession of, or is likely to come into the possession of, the data controller,
and includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual;

sensitive personal data means personal data consisting of information as to—
(a) the racial or ethnic origin of the data subject,
(b) his political opinions,
(c) his religious beliefs or other beliefs of a similar nature,
(d) whether he is a member of a trade union (within the meaning of the Trade Union and Labour Relations (Consolidation) Act 1992),
(e) his physical or mental health or condition,
(f) his sexual life,
(g) the commission or alleged commission by him of any offence, or
(h) any proceedings for any offence committed or alleged to have been committed by him, the disposal of such proceedings or the sentence of any court in such proceedings.

data controller means, subject to subsection (4), a person who (either alone or jointly or in common with other persons) determines the purposes for which and the manner in which any personal data are, or are to be, processed;

data processor in relation to personal data, means any person (other than an employee of the data controller) who processes the data on behalf of the data controller;

data subject means an individual who is the subject of personal data;

processing in relation to information or data, means obtaining, recording or holding the information or data or carrying out any operation or set of operations on the information or data, including—
(a) organisation, adaptation or alteration of the information or data,
(b) retrieval, consultation or use of the information or data,
(c) disclosure of the information or data by transmission, dissemination or otherwise making available, or
(d) alignment, combination, blocking, erasure or destruction of the information or data;

public authority means a public authority as defined by the Freedom of Information Act 2000 or a Scottish public authority as defined by the Freedom of Information (Scotland) Act 2002;

relevant filing system means any set of information relating to individuals to the extent that, although the information is not processed by means of equipment operating automatically in response to instructions given for that purpose, the set is structured, either by reference to individuals or by reference to criteria relating to individuals, in such a way that specific information relating to a particular individual is readily accessible.

Appendix B: Eight Principles in the Data Protection Act 1998

(UK Government, 1998) defines, and (Information Commissioner's Office, 2017) explains, the eight data protection principles as summarised below.

1) Personal data shall be processed fairly and lawfully. In practice, this means you must—
   (a) have legitimate grounds for collecting and using the personal data;
   (b) not use the data in ways that have unjustified adverse effects on the individuals concerned;
   (c) be transparent about how you intend to use the data, and give individuals appropriate privacy notices when collecting their personal data;
   (d) handle people's personal data only in ways they would reasonably expect; and
   (e) make sure you do not do anything unlawful with the data.
2) Personal data shall be obtained only for one or more specified and lawful purposes. In practice, this means you must—
   (a) be clear from the outset about why you are collecting personal data and what you intend to do with it;
   (b) comply with the Act's fair processing requirements, including the duty to give privacy notices to individuals when collecting their personal data;
   (c) comply with what the Act says about notifying the Information Commissioner; and
   (d) ensure that if you wish to use or disclose the personal data for any purpose that is additional to or different from the originally specified purpose, the new use or disclosure is fair.
3) Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed. In practice, this means you must—
   (a) only hold personal data about an individual that is sufficient for the purpose you are holding it for in relation to that individual; and
   (b) do not hold more information than you need for that purpose.
4) Personal data shall be accurate and, where necessary, kept up to date. In practice, this means you must—
   (a) hold personal data about an individual that is sufficient for the purpose you are holding it for in relation to that individual; and
   (b) do not hold more information than you need for that purpose.
5) Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes. In practice, this means you must—
   (a) only hold personal data about an individual that is sufficient for the purpose you are holding it for in relation to that individual; and
   (b) do not hold more information than you need for that purpose.
6) Personal data shall be processed in accordance with the rights of data subjects. The rights of individuals referred to are—
   (a) a right of access to a copy of the information comprised in their personal data;
   (b) a right to object to processing that is likely to cause or is causing damage or distress;
   (c) a right to prevent processing for direct marketing;
   (d) a right to object to decisions being taken by automated means;
   (e) a right in certain circumstances to have inaccurate personal data rectified, blocked, erased or destroyed; and
   (f) a right to claim compensation for damages caused by a breach of the Act.
7) Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data. In practice, this means there must be appropriate security to prevent the personal data being held from being accidentally or deliberately compromised. That is, you must—
   (a) design and organise your security to fit the nature of the personal data you hold and the harm that may result from a security breach;
   (b) be clear about who in your organisation is responsible for ensuring information security;
   (c) make sure you have the right physical and technical security, backed up by robust policies and procedures and reliable, well-trained staff; and
   (d) be ready to respond to any breach of security swiftly and effectively.
8) Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

Appendix C: Eight Rights in the General Data Protection Regulation

The General Data Protection Regulation (GDPR) (European Parliament, 2016) will apply in the UK from 25 May 2018. The GDPR defines eight rights that individuals have regarding the data being held about them, which are either new or strengthened rights with respect to the Data Protection Act (UK Government, 1998) as summarized above. Below is a summary of these rights as documented by the ICO (Information Commissioner's Office, 2017):

1) **The right to be informed**. Exactly what should be supplied to individuals and when is dependent on context (Information Commissioner's Office, 2017), but when provided it must be:
    (a) concise, transparent, intelligible and easily accessible;
    (b) written in clear and plain language, particularly if addressed to a child; and
    (c) free of charge.
2) **The right of access**. Under the GDPR, individuals will have the right to obtain:
    (a) confirmation that their data is being processed;
    (b) access to their personal data; and
    (c) other supplementary information – this largely corresponds to the information that should be provided in a privacy notice (see Article 15).
3) **The right to rectification**. Individuals are entitled to:
    (a) have personal data rectified if it is inaccurate or incomplete;
    (b) when their data is disclosed to third parties, inform the third party of the rectification (*and/or erasure*) where possible;
    (c) be informed about the third parties to whom their data has been disclosed to where appropriate.
4) **The right to erasure**. Individuals have a right to have personal data erased and to prevent processing in specific circumstances:
    (a) where the personal data is no longer necessary in relation to the purpose for which it was originally collected;
    (b) when the individual withdraws consent;
    (c) when the individual objects to the processing and there is no overriding legitimate interest for continued processing;
    (d) the personal data was unlawfully processed (i.e. otherwise in breach of the GDPR);
    (e) the personal data has to be erased in order to comply with a legal obligation;
    (f) the personal data is processed in relation to the offer of information society services to a child.

    Where a request for erasure can be refused for the following reasons:
    (a) to exercise the right of freedom of expression and information;
    (b) to comply with a legal obligation for the performance of a public interest task or exercise of official authority;
    (c) for public health purposes in the public interest;
    (d) archiving purposes in the public interest, scientific research historical research or statistical purposes; or
    (e) the exercise or defence of legal claims.
5) **The right to restrict processing**. You will be required to restrict the processing of personal data in the following circumstances:
    (a) where an individual contests the accuracy of the personal data, you should restrict the processing until you have verified the accuracy of the personal data;
    (b) where an individual has objected to the processing (where it was necessary for the performance of a public interest task or purpose of legitimate interests), and you are considering whether your organisation's legitimate grounds override those of the individual;
    (c) when processing is unlawful and the individual opposes erasure and requests restriction instead;
    (d) if you no longer need the personal data but the individual requires it to establish, exercise or defend a legal claim.
6) **The right to data portability**. Individuals have the right to obtain their personal data for their own purposes and potential reuse across different services. However, the right to data portability only applies:
    (a) to personal data an individual has provided to a controller;
    (b) where the processing is based on the individual's consent or for the performance of a contract; and
    (c) when processing is carried out by automated means.
7) **The right to object**. Individuals have the right to object to:
    (a) processing based on legitimate interests or the performance of a task in the public interest/exercise of official authority (including profiling);
    (b) direct marketing (including profiling); and

(c) processing for purposes of scientific/historical research and statistics.

Where you must stop processing the personal data unless:

(a) you can demonstrate compelling legitimate grounds for the processing, which override the interests, rights and freedoms of the individual; or

the processing is for the establishment, exercise or defence of legal claims