Data Protection Impact Assessment

June 2018

Scottish Government
Riaghaltas na h-Alba
gov.scot

Data Protection Impact Assessment (DPIA)

1. Introduction

The purpose of this document is to report on and assess any potential Privacy Impacts as a result of the introduction of legislation for an opt out system of deceased organ and tissue donation.

2. Document metadata

2.1 Name of Project: Human Tissue (Authorisation) (Scotland)Bill

Date of report: May 2018

2.2 Name of Information Asset Owner (IAO) of relevant business unit: Gareth Brown, Scottish Government Health Directorate

3. Description of the project

3.1 Description of the work:

The Bill will make provision for Scottish Ministers to establish and maintain a register enabling Scottish Ministers to secure effective performance of functions under section 1 of the 2006 Act[1]. In practice the Bill will introduce a statutory underpinning for the current arrangements between NHS Blood and Transplant who operate the NHS Organ Donor Register for the UK and the Scottish Government. The intention is that NHSBT would continue to maintain the Organ Donor Register on behalf of Scottish Ministers to ensure that organ and tissue donation continues to operate across the UK. NHSBT is a Special Health Authority for England and Wales responsible for managing the English Blood Service and Organ Donation services across the UK.

The Bill will provide a statutory basis in Scotland for declarations to be made to opt out of organ and tissue donation. This will mean that a person can opt out of organ and tissue donation by recording a decision on the Organ Donor Register. The organ donor register is a database holding personal information provided by individuals wishing to opt in to organ or tissue donation for transplantation after their death or opt out of such donation.

The provisions described above will not change the way the Organ Donor Register operates. The purpose of this Privacy Impact Assessment is to give assurance that the system is compliant with the principles of the Data Protection Act and General Data Protection Regulations.

[1] Human Tissue (Scotland) Act 2006

Personal data to be processed.

The Data will continue to be processed by NHS Blood and Transplant. People will continue to be able to register their authorisation to opt in or opt out of organ and tissue donation for transplantation in the same way as presently as follows:

- Organ donor registration websites (both the NHSBT's own website and the Organ Donation Scotland website managed by the Scottish Government)
- Registration phone line
- Paper based forms (opt in only)
- Driver and Vehicle Licensing Agency (opt in only)
- GP registration forms (opt in only)
- Boots advantage card (opt in only)

The data collected is:

- NHS/CHI number

Mandatory Personal data collected is:

- Full name
- Address
- Postcode
- Gender – A person can also select 'Prefer not to say'
- Date of Birth
- Donation decision and choices

Additional non mandatory information which may be collected, depending on registration method used is

- Telephone number
- Mobile number
- E-mail address
- Preferred form of contact
- Ethnic classification
- Religion
- Source of registration
- Marketing campaign id
- Consent flag for data protection
- Death status – checks are used to ensure the register is up to date and remove those who are deceased
- Date of death

The following personnel have access to the register:

- ODR call centre staff for the purposes of adding information given by an individual over the telephone or to confirm details held.

- Sub-contractors of NHSBT who handle paper registrations and enter the data onto the ODR
- National Transplant Liaison Co-ordinators of NHSBT who access the system on behalf of Specialist Nurses for Organ Donation
- Specialist Nurses for Organ Donation at the appropriate time of end of life care
- Tissue nurses to facilitate tissue transplantation
- The ODR Team to process registrations and improve the quality and accuracy of data held on the ODR
- NHSBT Statistics for analysis and reporting purposes

An Access Control Procedure is in place to ensure all personal who have access to the register are appropriately trained, and have the appropriate access level.

All data is encrypted and backed up by NHSBT or by subcontractors responsible for hosting the data.

NHSBT owns the data; The Information Asset Owner is Alex Hudson, Head of the NHS Organ Donor Register.

Electronic records are sent via secure file transfer protocol (sFTP) using XML files. Mailing files are sent to GI Solutions in CSV format.

3.2 Explain the legal basis for the sharing with internal or external partners:

The following basis applies to the processing of the mandatory personal data included on the ODR:
(a) Consent: the individual has given clear consent for you to process their personal data for a specific purpose.
If the Human Tissue (Authorisation) (Scotland) Bill is approved by the Scottish Parliament, once the relevant provisions are commenced, the following basis will instead be relied upon:
(c) Legal obligation: the processing is necessary for you to comply with the law (not including contractual obligations) and/or
(e) Public task: the processing is necessary for you to perform a task in the public interest or for your official functions, and the task or function has a clear basis in law.
The following basis applies to the processing and sharing of special category data:

Article 9(2)(a) the data subject has given explicit consent to the processing of those personal data for one or more specified purposes, except where Union or Member State law provide that the prohibition referred to in paragraph 1 may not be lifted by the data subject.

The Human Tissue (Scotland) Act 2006, the Human Tissue Act 2004 and the Human Transplantation (Wales) Act 2013 require those carrying out donation and transplant activities to satisfy themselves that the donation and transplantation of organs and

tissue can proceed within the requirements of the law. This means satisfying themselves that the appropriate authorisation for donation and transplantation is in place and involves access to information on the Organ Donor Register as to whether a person had recorded an authorisation to donate or not to donate for the purpose of transplantation.
The law also provides that in certain circumstances a nearest relative (nearest relative is defined in s. 50 of the 2006 Act) can authorise donation. For this to happen the Specialist Nurse for Organ Donation or Tissue Donor Coordinator has to provide information to the effect that a person has registered a decision or not on the organ donor register. In cases where a person has authorised donation on the ODR their nearest relatives also needs to be advised so that the donation process can be explained to them and they can assist in providing necessary background information about the potential donor to assist with the process.

4. Stakeholder analysis and consultation

4.1 List all the groups involved in the project, and state their interest.

Group	Interest
NHS Blood and Transplant	Responsible for the maintenance and management of the UK Organ Donor Register
NHS National Services Scotland, Scottish National Blood Transfusion Service	Responsible for tissue donor services in Scotland and tissue donor co-ordinator services. Access to the ODR

4.2 Method used to consult with these groups when making the PIA.

4.3 Method used to communicate the outcomes of the PIA .

5. Questions to identify privacy issues

5.1 Involvement of multiple organisations

External Partners – Allow individuals to join the ODR

Boots
GP Surgeries /NHS Digital
Scottish Organ Donation Website

External partners – Subcontractors

APS Group (GI Solutions) – Mailing Service, providing confirmation letters to registrants
Teleperformance – Organ Donor Helpline, checking and amending registrations, providing advice on Organ Donation to callers
NHS National Services Scotland – Scottish CH1 number batch tracing service
Automated Document Solutions – Manual input of paper registration forms
Northgate – IT development and maintenance contract for the bespoke ODR system

5.2 Anonymity and pseudonymity

The information held on the register is not anonymous. It is however, only accessible to the appropriate authorised individuals.

5.3 Technology

No personal data is gathered as a by-product of the ODR.

5.4 Identification methods

Unique identifiers are collected as part of an ODR registration. See section 3.2.

5.5 Sensitive/Special Category personal data

Special category data is sometimes collected as part of an ODR registration (e.g. where the person provides their ethnic origin or religion). See section 3.2

5.6 Changes to data handling procedures

Paper ODR Registration Forms
Sent directly to the ODR Team via pre-marked envelope (in most cases)
Stored in lockable cabinets
When mailed in bulk, sent via courier service.
Retained for one week after processing and then destroyed via NHSBT confidential waste procedures. An exception applies for a sample of forms used for sample checking purposes. These will be retained for up to four weeks before being destroyed.

Electronic records
Sent via sFTP using XML files. Mailing files sent to GI Solutions are sent in CSV format. Occasionally sent via secure e-mail (business continuity when sFTP unavailable).

ODR Database
Records are stored on the Microsoft Azure Cloud (NHSBT subscription)
Read only and write access processes in place and limited to a need to know basis
Role-based access catering for multiple different user groups.

5.7 Statutory exemptions/protection

N/A

5.8 Justification

N/A

5.9 Other risks

System testing

Currently the test environment is a copy of the live environment. Future ambitions are to continue to utilise real data but to ‘scramble’ and anonymise the personal identifiable information within the test environments.

6. The Data Protection Act (DPA) and General Data Protection Regulation (GDPR) Principles

Principle	**Compliant –** Yes/No	**Description of how you have complied**
6.1 DPA Principle 1 and GDPR Principle 1 – fair and lawful, and meeting the conditions for processing	YES	NHSBT Privacy notice www.nhsbt.nhs.uk/privacy/
Principle	**Compliant – Yes/No**	**Description of how you have complied**
6.2 DPA Principle 2 and GDPR Principle 2 – purpose limitation	YES	Information only used for the purposes of including data on ODR
Principle	**Compliant – Yes/No**	**Description of how you have complied**
6.3 DPA Principle 3 and GDPR Principle 3 – adequacy, relevance and data minimisation	YES	Role based access to data on ODR, unique reference number used in place of identifiable data wherever possible
Principle	**Compliant – Yes/No**	**Description of how you have complied**
6.4 DPA Principle 4 and GDPR Principle 4 – accurate, kept up to date, deletion	YES	Data integrity audits
Principle	**Compliant – Yes/No**	**Description of how you have complied**
6.5 DPA Principle 5 and GDPR Principle 5 – kept for no longer than necessary, anonymization	YES	NHS minimum retention periods
Principle	**Compliant – Yes/No**	**Description of how you have complied**
6.6 DPA Principle 6 and GDPR Articles 12-22 – data subject rights	YES	Compliant with all including the right to be forgotten on ODR
Principle	**Compliant – Yes/No**	**Description of how you have complied**
6.7 DPA Principle 7 and GDPR Principle 6 - security	YES	Role based access, regular audits and contracts and/or information sharing agreements in place with all third parties
Principle	**Compliant – Yes/No**	**Description of how you have complied**
6.8 DPA Principle 8 and GDPR Article 24 - Personal data shall not be transferred to a country or territory outside the European Economic Area.	N/A	Data from ODR not processed outside the UK

7. Risks identified and appropriate solutions or mitigation actions proposed

Is the risk eliminated, reduced or accepted?

Risk	Ref	Solution or mitigation	Result
Paper registration form processing is contracted out to a supplier – they have data storage centres outside of the European Economic Area (EEA).	1	All data is transferred securely via SFTP in accordance with IT Security procedures. This information is communicated to registrants in the data privacy statement. Sample checking is completed.	Reduce
Data is shared with external partners such as a mailing house	2	All data is transferred securely via SFTP in accordance with IT Security procedures. A data sharing agreement is in place.	Reduce

8. Incorporating Privacy Risks into planning

Explain how the risks and solutions or mitigation actions will be incorporated into the project/business plan, and how they will be monitored. There must be a named official responsible for addressing and monitoring each risk.

Risk	Ref	How risk will be incorporated into planning	Owner
As above – Ref 1	1	Investigating alternative options for paper form processing - CONFIDENTIAL	ODR Team
As above – Ref 2	2	Update data sharing agreements to comply with GDPR.	ODR Team

Risk	Ref	How risk will be incorporated into planning	Owner
As above	1		

9. Authorisation and publication -

The PIA report should be signed by your Information Asset Owner (IAO). The IAO will be the Deputy Director or Head of Division.

Before signing the PIA report, an IAO should ensure that she/he is satisfied that the impact assessment is robust, has addressed all the relevant issues and that appropriate actions have been taken.

By signing the PIA report, the IAO is confirming that the impact of applying the policy has been sufficiently assessed against the individuals' right to privacy.

The results of the impact assessment must be published in the eRDM with the phrase "Privacy Impact Assessment (PIA) report" and the name of the project or initiative in the title.

Details of any relevant information asset must be added to the Information Asset Register, with a note that a PIA has been conducted.

I confirm that the impact of the relevant provisions of the Human Tissue (Authorisation) (Scotland) Bill has been sufficiently assessed against the needs of the privacy duty:

Name and job title of a IAO or equivalent	**Date each version authorised**
Gareth Brown, Deputy Director, Scottish Government, Health Protection Division	24 May 2018

This publication is available at **www.gov.scot**

Any enquiries regarding this publication should be sent to us at
The Scottish Government
St Andrew's House
Edinburgh
EH1 3DG

ISBN: 978-1-78851-939-7 (web only)

Published by The Scottish Government, June 2018

Produced for The Scottish Government by APS Group Scotland, 21 Tennant Street, Edinburgh EH6 5NA
PPDAS422586 (06/18)