D4.1 Webpage with materials of the workshop on data privacy standards

Grant Agreement number: 881553
Project acronym: SAVDON
Work Package number: WP1

Periodic report: 1st □ 2nd □ 3rd X 4th □

Period covered: from 01st January to 31st December 2020

Organisation: **World Marrow Donor Association (WMDA)**
LEAR: Lydia Foeken
Project coordinator: Lydia Foeken
Tel: 0031 88 505 7900
E-mail: lydia.foeken@wmda.info
Organisation website address: www.wmda.info

Co-funded by
the Health Programme
of the European Union

"This Deliverable D4.1 of an activity received funding under an operating grant from the European Union's Health Programme (2014-2020)."

Table of Contents

Introduction

The World Marrow Donor Association (WMDA) community maintains a uniquely large and diverse genetic dataset. Ever since the WMDA started maintaining this unique dataset, one of the main focusses has always been to treat this highly sensitive data as careful as possible.

WMDA's dataset brings great opportunities to save lives; however, in the current society it brings even bigger responsibilities due to the increasing interest in medical and genetic information by cybercriminals. Privacy regulators are responding to this interest by applying increasing restrictions to better protect private data, giving an increased difficulty for members to keep an oversight of all regulations. An example is the General Data Protection Regulation (GDPR) of 2018 all EU member states are bound by.

To support the membership, the WMDA Security and Privacy Committee (WMDA-SPC) organised a workshop for all members during the online WMDA semi-annual meeting in June 2020. This workshop aimed to give the membership a roadmap to comply with all data privacy regulations and keep data as safe as possible.

Data protection workshop

The WMDA data security workshop was planned as part of the semi-annual WMDA membership meeting. Unfortunately, COVID-19 made it impossible to hold a physical WMDA membership meeting. This made it difficult to give a qualitative workshop on data security as online webinars make it significantly harder to interact with the audience.

In order to still organise a highly qualitative data security workshop, the WMDA went above and beyond to reorganise its semi-annual membership meeting in a virtual way, where the easy accessibility of interaction during the workshop was maintained. The workshop consisted out of two parts.

First part being a plenary part with key information on data security and the presentation of the novel Data Security Peer Consultation Programme, followed by an explanation on the importance of this roadmap to protect the highly sensitive data of the WMDA members. During this plenary part, participants had the opportunity to send questions to one central moderator. This made sure that this part with all the key information was not interrupted, and all questions could be answered at an appropriate timing. The ability to ask questions even during the presentation caused an increased participation and made that the amount of questions asked were on par with previous meetings.

During the second part, participants could give their opinion on the proposed Data Security Peer Consultation Programme, share their concerns on the newly presented programme, and indicate whether they supported this programme or not and why they did so. This valuable feedback could then be used to improve the Data Security Peer Consultation Programme.

Workshop contents

Importance Data Security Peer Consultation Programme

The main purpose of the data security workshop was to introduce and get the WMDA members familiar with the Data Security Peer Consultation Programme. The programme is set up as a community effort to raise the compliance bar by helping each other. The key to a successful community effort is for the membership to have the ability to effortlessly give their opinion on the programme. The community input makes that the programme is easily accessible for all members, as members can give feedback if something is not well implementable. The membership input prevents the chance of regulations being overlooked significantly.

Registries' and WMDA's primary goal are to help patients find a suitable donor and with this comes the obligation to protect the privacy of its donors. With more and more donors becoming available, registries should weigh risks of potential privacy violations, while the community as a whole should take efforts towards continuously improving privacy security and protection.

To increase the consciousness around privacy security and protection, WMDA initiated the Data Security Peer Consultation Programme. In contrast to an audit, the idea of a peer consultation review is to regularly (self-)assess the status of a registry with regards to best practice, relevant regulations and standards in comparison to others on the one hand and the community needs as a whole on the other. In addition, a regular review by peers will enhance learning from experience and the adoption of best practices. This way the bar will be raised naturally by mutually beneficial cooperation.

The Data Security Peer Consultation Programme aims to complement the WMDA accreditation programme with individual privacy rights. As not all WMDA member organisations are WMDA accredited yet, the peer consultation tool is a tool that registries can use that are not WMDA accredited. The Data Security Peer Consultation Programme helps non-WMDA accredited organisations to cope with the data security regulations.

Implementation of the Data Security Peer Consultation Programme

The WMDA-Security Privacy Committee developed a questionnaire (Appendix 1) based on current best practices and applicable regulations. The scope of the questionnaire is limited to the following regulations, but continues to improve and comply with even more regulations:

- General Data protection Regulation 2016/2017 (EU) (https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679&from=EN#d1e40-1-1)
- USA various state, national and sector privacy laws (https://iclg.com/practice-areas/data-protection-laws-and-regulations/usa)
- The Australian Privacy Act (https://www.oaic.gov.au/privacy/the-privacy-act/)

As the regulations named above are known complete regulation, most other local regulations might be largely compatible. Please note that US Law does not have a harmonized federal privacy law, so that sector laws and state laws as applicable must be considered. Each question in the questionnaire will be related to parts of the regulations which are in scope. Members may help upgrading the questionnaire by adding their own applicable regulations.

In order to keep for members up to date with the ever-changing regulations, members should complete or review the questionnaire once per year and have it reviewed by a peer member upon completion and whenever updates are files. The peer member may ask for evidence and will discuss its findings with the member under review. Preferably the reviewing member should be invited by its peer to assess its findings on-site to enhance the learning process, the costs of which should be borne by the registry under review. Typically, the review process should not be considered as an audit, but merely as a consultation process. The reviewer cannot be consulted by third parties or held liable in any way: each registry is responsible and held accountable for its own responses.

The review should be filed at the WMDA share website in the registry's file, accessible for WMDA members and should be updated whenever a registry deems it appropriate in view of upgrades of its status. Each third year a different registry will review the questionnaire and reviewed registries should not assess the reviewing registry within the 3-year time frame. In addition, registries can only be reviewed by registries which already underwent a review themselves. In the event that the registry already undergoes an independent, third party, comprehensive evaluation of the registry's compliance to applicable security and privacy regulations, that registry can supply an overview of the assessment methodology and results. In those cases, the registry will not be required to reperform the same control assessment with a peer registry.

Feedback Data Security Peer Consultation Programme after the workshop

The second part of the workshop consisted of a discussion on the newly presented questionnaire. A vast majority of the 50 participants showed support for the Data Security Peer Consultation Programme as a complement to the already existing WMDA standards. Some members did indicate that they would also be happy to see this questionnaire being added to the WMDA standards in the long run and be a requirement for the WMDA accreditation in order to increase the membership's data security and quality. This is something the WMDA will keep in mind as it continues to develop and improve the Data Security Peer Consultation Programme.

For 2021 the template form will be expanded to include transplant centres and donor centres as well, so that these organisations can also be reviewed.

Webpage with workshop materials

To assist the membership with complying with data privacy standards, the WMDA started hosting a designated page featuring the information and questionnaire from the June 2020 workshop (screenshots of the webpages in Appendix 2, https://share.wmda.info/x/bpGbEw). The page gives a clear overview on the different data privacy standards processed in the Data Security Peer Consultation Programme and why it is important to comply with these. The page exists out of 4 pillars.

The first pillar describes the importance of the GDPR the EU is using and what WMDA members have to do in order to comply with this regulation. It summarizes all necessary actions to comply with the GDPR and gives examples on how other organisations made sure to comply with the GDPR. The first pillar also states common misconceptions about sensitive donor information and why these statements are invalid.

The second pillar stresses the importance of a mandatory Data Protection Officer for every accredited registry. It explains why a Data Protection Officer is mandatory for every accredited registry, which specifications a Data Protection Officer should meet, and what the position of a Data Protection Officer should be inside an organisation.

The third pillar explains all WMDA member organisations have to sign two data use agreements, links to the respective agreements, and links to a page with an overview of registries that have signed the data use agreements already. One agreement is for the exchange of data with WMDA, and a second agreement is for the exchange of data with other WMDA member organisations.

The fourth pillar stresses the requirement of a Written Information Security Policy (WISP) for WMDA accredited member organisations. To help member organisations set up a WISP, the fourth pillar links to several examples of other WMDA members to use as a template.

Appendix 1: Peer Review Questionnaire

REGISTRY NAME: ……..

ION : ……..

The registry holds the following accreditations:

o WMDA accreditation

o ISO 27001 or ISO 27018

o …… (local accreditation), related to ISO 27001 or ISO 27018

#	Subject	Check if compliant	GDPR	AU Privacy Act	US DPR
1	**Subject Consent**		**II**		
1.1.	Does the registry have adequate procedures in place to ask, store and retrieve consent from donors from who it collects personal information and for who it acts in the capacity of data controller?	o	II.7		§164.502
1.2.	In case the registry acts as a co-controller for the collection of patient data: does it have adequate procedures in place to ask, store and retrieve consent from patients or the assurance that the transplant centre obtains, stores and retrieves such consent?	o	II.7	APP 11	§164.502
1.4.	Does the donor's consent encompass portability to other registries and WMDA to allow matching with patients?	o	III.20	APP 8	§164.502
1.5.	Is all collected information sufficiently specified and explained in the registry's consent forms?	o	II.9	APP 1	§164.502

#	Subject	Check if compliant	GDPR	AU Privacy Act	US DPR
1.6.	Does the registry's state law allow exemption for medical and/or other sensitive data collected?	o	II.9.2a	APP 8	§164.502
2	**Information and access to personal data**		**III.S2**		
2.1.	Does the registry have procedures in place to confirm the collection of personal data at the time when personal data are obtained and does such confirmation include: • contact details of the registry • the purpose of the processing for which the personal data are intended and other details provided in the donor or patient's consent or a reference to that consent • details about the period for which the data are stored • the right to access or erase personal data • the right to lodge a complaint with a supervisory authority	o	III.13.1	APP 10	
2.2.	Does the registry have procedures in place to provide access to personal data to donors within one month after receipt of a request thereto?	o	III.15	APP 12	45 CFR 164.524
3	**Rectification and erasure of personal data**		**III.S3**		
3.1.	Does the registry have procedures in place for donors to rectify personal information, either by direct access or a request?	o	III.16	APP 13	NA
3.2.	Does the registry have procedures in place to erase personal data or anonymize donor records in such way that the donor can no longer be identified at the donor's request?	o	III.17	APP 1	NA

#	Subject	Check if compliant	GDPR	AU Privacy Act	US DPR
3.3.	Does the registry have procedures in place to erase personal data or anonymize donor records in such way that the donor can no longer be identified when the donor no longer fulfils the criteria for being registered?	o	III.18	APP 1	NA
3.4.	In case of the action described under 3.3.: does the donor receive notification of the erasure?	o	III.19	APP 10	NA
4	**Data processing responsibilities**		**IV.S1**		
4.1.	Does the registry have data processing agreements or co-controlling arrangements in place with and of the following third parties to whom personal or pseudonymized data is provided: • WMDA • Donor centres whose donors are requested on behalf of local transplant centres • Transplant centres	o	IV.24 IV.26 IV.28	APP 8	§164.502(e)(1)(ii)
4.2.	Does the registry comply with requirements for controllers or processors outside the European Union?	o	IV.27	APP 8	
5	**Data security and data breach provisions**		**IV.S2**		
5.1.	Does the registry have a written information security policy in place?	o			
5.2.	Does the registry have adequate security measures in place to protect personal data, to include but not limited to: • Regular penetration testing and a record of remedial action based on the findings of such testing	o	IV.32	APP 11	§164.308 §164.310

#	Subject	Check if compliant	GDPR	AU Privacy Act	US DPR
					§164.312
5.3.	Is a procedure in place to notify the supervisory authority or the data controller in case of a personal data breach within the limits as the regulations or the data processing agreements require?	o	IV.33	APP 11	§ 164.410(a)(1)
5.4.	Is a procedure in place to notify the donor in case of a personal data breach within the limits as the regulations or the data processing agreements require?	o	IV.34	APP 11	§ 164.410 - 414
5.5.	Does the registry have examples of such notifications and can it demonstrate compliance with the regulations in these cases?	o	IV.33 IV.34	APP 11	?
6	**Data protection impact assessment**		**IV.S3**		
6.1.	Does the registry have procedures in place to assess and classify security risks, including but not limited to: • Environmental incidents, acts of God • Hardware failure • Physical access to data	o	IV.35	APP 11	§164.308(a)(1)(ii)(A)
6.2.	Does the registry have adequate backup procedures, to include: • data mirroring to prevent interruption of operations in case of hardware failure • complete recovery of the systems environment for a limited period • procedures to restore data and testing thereof • interval backup's	o	IV.35	APP 11	§164.308(a)(7)(ii)(A)

#	Subject	Check if compliant	GDPR	AU Privacy Act	US DPR
7	**Data Protection Officer**		**IV.S4**		
7.1.	Did the registry appoint a Data Protection Officer in compliance with local regulations?	o	IV.37	APP 1	45 CFR 164.308

This questionnaire is reviewed by: …… (Registry name), …….. (ION number)

The reviewing registry has been able to properly review the registry assessment and declares that its findings are compliant with it.

<Place>, <Date>

Signed on behalf of the reviewed registry

Signed on behalf of the reviewing registry

Appendix 2: Webpage with workshop materials

Security & Privacy - GDPR

Created by Paulien Kort, last modified by Kiet Foeken just a moment ago

Introduction

As medical and genetic information continues to become more valued by cybercriminals, privacy regulators are responding by applying increasing restrictions on the cybersecurity and cross-border data export protections applied to personal information. As the WMDA community maintains a uniquely large and diverse genetic dataset, this changing landscape presents new risks to WMDA member organisations and must be managed closely. To support the membership, cyber risk experts within the WMDA have launched a WMDA Security and Privacy Committee to aid members in cyber risk education and the practical application of cyber risk best practices. The WMDA Security and Privacy Committee created a questionnaire to help WMDA members comply with privacy regulations.

European Data Protection Regulation (GDPR)

A new EU privacy law, the General Data Protection Regulation (GDPR), is set to replace the prior EU Data Protection Directive 95/46/ec, effective May 25, 2018. GDPR establishes a harmonized set of privacy obligations for the "processing" (performance of any "operation" on personal data, for example, collection, organisation, storage, alteration, or use) of the personal data of European residents. With regard to third party data processing of personal data, GDPR expands significantly upon an organisation's responsibility for overseeing its third-party processing activities and sets out specific rules for allocating responsibility between the organization and its third-party data processors. All WMDA member organisations that collect or process European personal data will likely need to take action.

- GDPR-ready third party data processing contract clauses
- GDPR-ready donor consent agreement template
- GDPR-ready website privacy policy for donors
- GDPR readiness assessment tracking tool

Webpage with workshop materials – continued

Top Misunderstandings of the General Data Protection Regulation (GDPR)

1. My registry is located outside of the European Union. GDPR does not apply.

Fact - GDPR applies to any organization that receives personal information of a European resident, no matter where the organization is located or where the European resident is located. Since stem cell supply chains traverse the globe, it is likely that all registries accepting European donors are processing personal data of European residents and impacted by GDPR.

2. My registry doesn't collect personal data from any European resident. GDPR does not apply.

Fact - One major change of the new GDPR from the previous EU Privacy Directive is the obligations it imposes on third party and foreign data processors. While the expanded donor consent requirements are limited to the registries that directly collect personal information and biological sample from the donor, foreign registries will need to meet specific security requirements (enforced by contract) before the European registry can share their donors' data. Non-European registries should ensure their able to comply with these requirements to avoid disruption in their ability to receive EU personal data. Additional data export/import requirements may apply to registries where the European Union has deemed certain countries to have inadequate privacy laws.

3. The personal data my registry receives is de-identified. GDPR does not apply.

Fact - The GDPR has broadly defined Personal Data as "any information relating to an identified or identifiable natural person." GDPR makes it clear that personal data that is linkable through one or more factors, such as through a unique Donor ID number, remains within the GDPR jurisdiction. While the donor and patient personal attributes must be minimized (formally called pseudonimization), the remaining donor record remains linkable. Consequently, registries that receive minimized donor records from European registries are not exempt from the regulation.

4. Hackers don't care about this type of data.

Fact - Hackers are finding new and creative ways to monetize medical information for short-term financial gain or long-term national strategic advantages. The volume and diversity of the WMDA donor inventory could present a unique opportunity to motivated cyber criminals. The WMDA community is responsible for providing adequate cyber defenses and data governance to protect the personal information entrusted to us and ensure the long-term sustainability of cross-border cell transplants.

Webpage with workshop materials - continued

Data Protection Officer - DPO

Registries need to develop an internal record keeping requirements, and a DPO appointment will be mandatory only for those controllers and processors whose core activities consist of processing operations which require regular and systematic monitoring of data subjects on a large scale or of special categories of data or data relating to criminal convictions and offences. Importantly, the DPO:

- Must be appointed on the basis of professional qualities and, in particular, expert knowledge on data protection law and practices
- May be a staff member or an external service provider
- Contact details must be provided to the relevant data protection authorities
- Must be provided with appropriate resources to carry out their tasks and maintain their expert knowledge
- Must report directly to the highest level of management
- Must not carry out any other tasks that could results in a conflict of interest

Listing of international donors and cord blood units - sign two data use agreements

To participate in the international data-exchange of donor data, all WMDA member organisations are obliged to sign two data use agreements. The first data use agreement is for exchange of data with WMDA, the second data use agreement is for exchange of data with other WMDA member organisations.

Find here the explanation about the agreement to be signed with WMDA.

- Agreement to be signed with WMDA
- Agreement facilitated by WMDA: registry-to-registry agreement

Webpage with an overview of registries that have signed the data use agreement, click here.

Written Information Security Policies

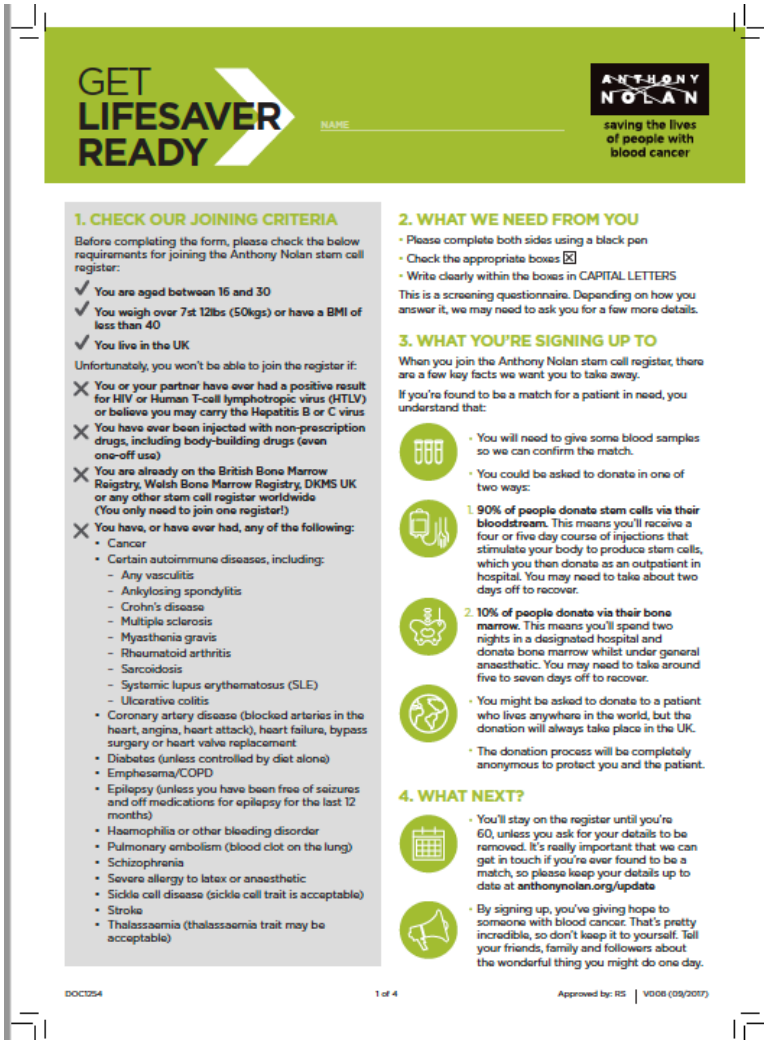
WMDA Standards require that each has implemented a written information security policy (WISP). You can download here examples of WMDA member organisations, that you can use as a template.

- Australian draft policy
- Example of Australian University
- Example of table of contents from different size of registries
- Example of NMDP
- Example of ZKRD

Data breach - how to inform all WMDA member organisations

WMDA has a distribution list of all Data Protection Officers in WMDA member organisations. You can find the list here.

GDPR Ready Donor consent agree template



GET LIFESAVER READY

NAME

ANTHONY NOLAN
saving the lives of people with blood cancer

1. CHECK OUR JOINING CRITERIA

Before completing the form, please check the below requirements for joining the Anthony Nolan stem cell register:

- ✓ **You are aged between 16 and 30**
- ✓ **You weigh over 7st 12lbs (50kgs) or have a BMI of less than 40**
- ✓ **You live in the UK**

Unfortunately, you won't be able to join the register if:

- ✗ **You or your partner have ever had a positive result for HIV or Human T-cell lymphotropic virus (HTLV) or believe you may carry the Hepatitis B or C virus**
- ✗ **You have ever been injected with non-prescription drugs, including body-building drugs (even one-off use)**
- ✗ **You are already on the British Bone Marrow Reigstry, Welsh Bone Marrow Registry, DKMS UK or any other stem cell register worldwide (You only need to join one register!)**
- ✗ **You have, or have ever had, any of the following:**
  - Cancer
  - Certain autoimmune diseases, including:
    - Any vasculitis
    - Ankylosing spondylitis
    - Crohn's disease
    - Multiple sclerosis
    - Myasthenia gravis
    - Rheumatoid arthritis
    - Sarcoidosis
    - Systemic lupus erythematosus (SLE)
    - Ulcerative colitis
  - Coronary artery disease (blocked arteries in the heart, angina, heart attack), heart failure, bypass surgery or heart valve replacement
  - Diabetes (unless controlled by diet alone)
  - Emphesema/COPD
  - Epilepsy (unless you have been free of seizures and off medications for epilepsy for the last 12 months)
  - Haemophilia or other bleeding disorder
  - Pulmonary embolism (blood clot on the lung)
  - Schizophrenia
  - Severe allergy to latex or anaesthetic
  - Sickle cell disease (sickle cell trait is acceptable)
  - Stroke
  - Thalassaemia (thalassaemia trait may be acceptable)

2. WHAT WE NEED FROM YOU

- Please complete both sides using a black pen
- Check the appropriate boxes ☒
- Write clearly within the boxes in CAPITAL LETTERS

This is a screening questionnaire. Depending on how you answer it, we may need to ask you for a few more details.

3. WHAT YOU'RE SIGNING UP TO

When you join the Anthony Nolan stem cell register, there are a few key facts we want you to take away.

If you're found to be a match for a patient in need, you understand that:

- You will need to give some blood samples so we can confirm the match.
- You could be asked to donate in one of two ways:

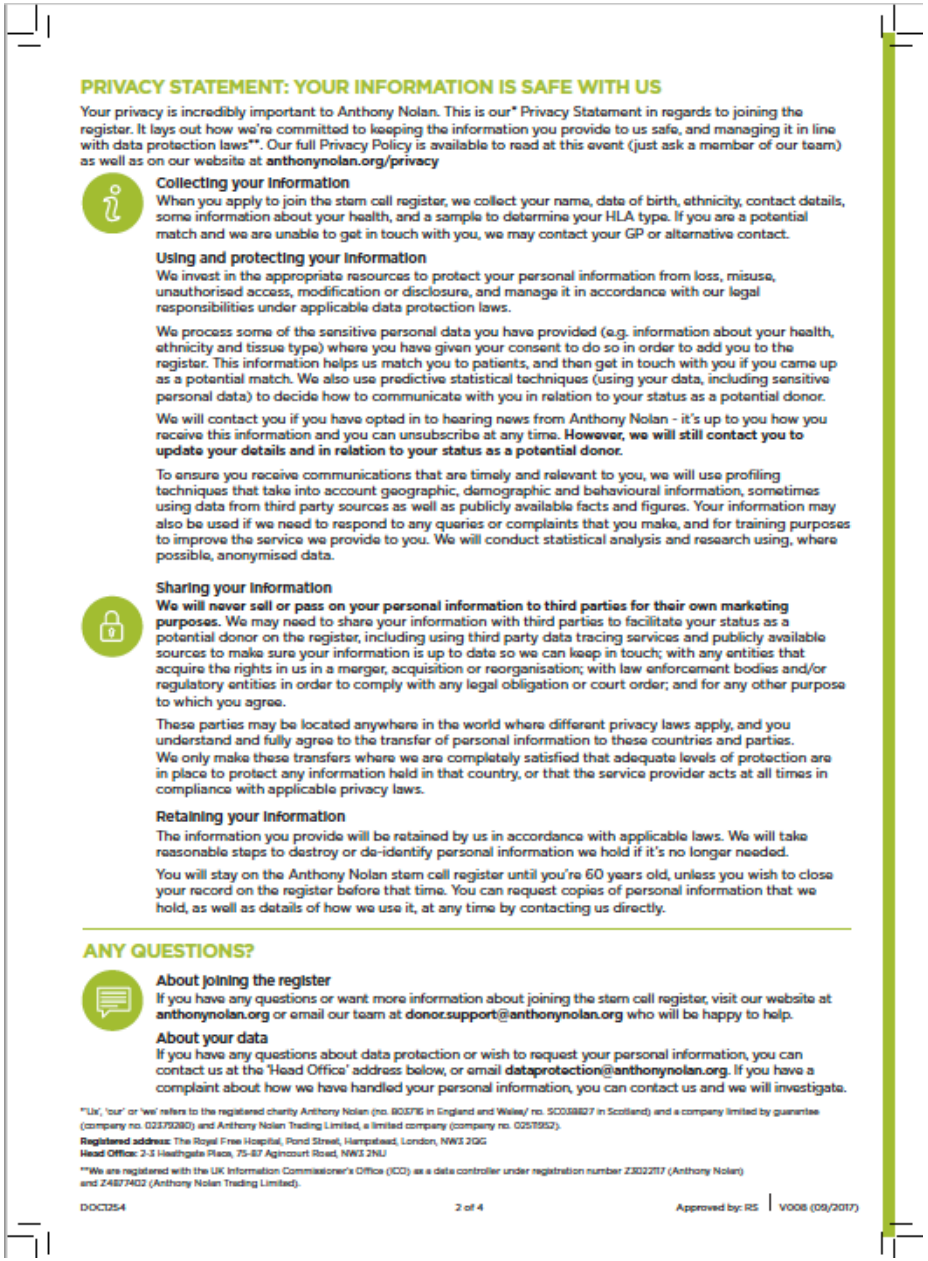
1. **90% of people donate stem cells via their bloodstream.** This means you'll receive a four or five day course of injections that stimulate your body to produce stem cells, which you then donate as an outpatient in hospital. You may need to take about two days off to recover.
2. **10% of people donate via their bone marrow.** This means you'll spend two nights in a designated hospital and donate bone marrow whilst under general anaesthetic. You may need to take around five to seven days off to recover.

- You might be asked to donate to a patient who lives anywhere in the world, but the donation will always take place in the UK.
- The donation process will be completely anonymous to protect you and the patient.

4. WHAT NEXT?

- You'll stay on the register until you're 60, unless you ask for your details to be removed. It's really important that we can get in touch if you're ever found to be a match, so please keep your details up to date at **anthonynolan.org/update**
- By signing up, you've giving hope to someone with blood cancer. That's pretty incredible, so don't keep it to yourself. Tell your friends, family and followers about the wonderful thing you might do one day.

DOC1254 1 of 4 Approved by: RS | V008 (09/2017)



PRIVACY STATEMENT: YOUR INFORMATION IS SAFE WITH US

Your privacy is incredibly important to Anthony Nolan. This is our* Privacy Statement in regards to joining the register. It lays out how we're committed to keeping the information you provide to us safe, and managing it in line with data protection laws**. Our full Privacy Policy is available to read at this event (just ask a member of our team) as well as on our website at **anthonynolan.org/privacy**

Collecting your information

When you apply to join the stem cell register, we collect your name, date of birth, ethnicity, contact details, some information about your health, and a sample to determine your HLA type. If you are a potential match and we are unable to get in touch with you, we may contact your GP or alternative contact.

Using and protecting your information

We invest in the appropriate resources to protect your personal information from loss, misuse, unauthorised access, modification or disclosure, and manage it in accordance with our legal responsibilities under applicable data protection laws.

We process some of the sensitive personal data you have provided (e.g. information about your health, ethnicity and tissue type) where you have given your consent to do so in order to add you to the register. This information helps us match you to patients, and then get in touch with you if you came up as a potential match. We also use predictive statistical techniques (using your data, including sensitive personal data) to decide how to communicate with you in relation to your status as a potential donor.

We will contact you if you have opted in to hearing news from Anthony Nolan - it's up to you how you receive this information and you can unsubscribe at any time. **However, we will still contact you to update your details and in relation to your status as a potential donor.**

To ensure you receive communications that are timely and relevant to you, we will use profiling techniques that take into account geographic, demographic and behavioural information, sometimes using data from third party sources as well as publicly available facts and figures. Your information may also be used if we need to respond to any queries or complaints that you make, and for training purposes to improve the service we provide to you. We will conduct statistical analysis and research using, where possible, anonymised data.

Sharing your information

We will never sell or pass on your personal information to third parties for their own marketing purposes. We may need to share your information with third parties to facilitate your status as a potential donor on the register, including using third party data tracing services and publicly available sources to make sure your information is up to date so we can keep in touch; with any entities that acquire the rights in us in a merger, acquisition or reorganisation; with law enforcement bodies and/or regulatory entities in order to comply with any legal obligation or court order; and for any other purpose to which you agree.

These parties may be located anywhere in the world where different privacy laws apply, and you understand and fully agree to the transfer of personal information to these countries and parties. We only make these transfers where we are completely satisfied that adequate levels of protection are in place to protect any information held in that country, or that the service provider acts at all times in compliance with applicable privacy laws.

Retaining your information

The information you provide will be retained by us in accordance with applicable laws. We will take reasonable steps to destroy or de-identify personal information we hold if it's no longer needed.

You will stay on the Anthony Nolan stem cell register until you're 60 years old, unless you wish to close your record on the register before that time. You can request copies of personal information that we hold, as well as details of how we use it, at any time by contacting us directly.

ANY QUESTIONS?

About joining the register

If you have any questions or want more information about joining the stem cell register, visit our website at **anthonynolan.org** or email our team at **donor.support@anthonynolan.org** who will be happy to help.

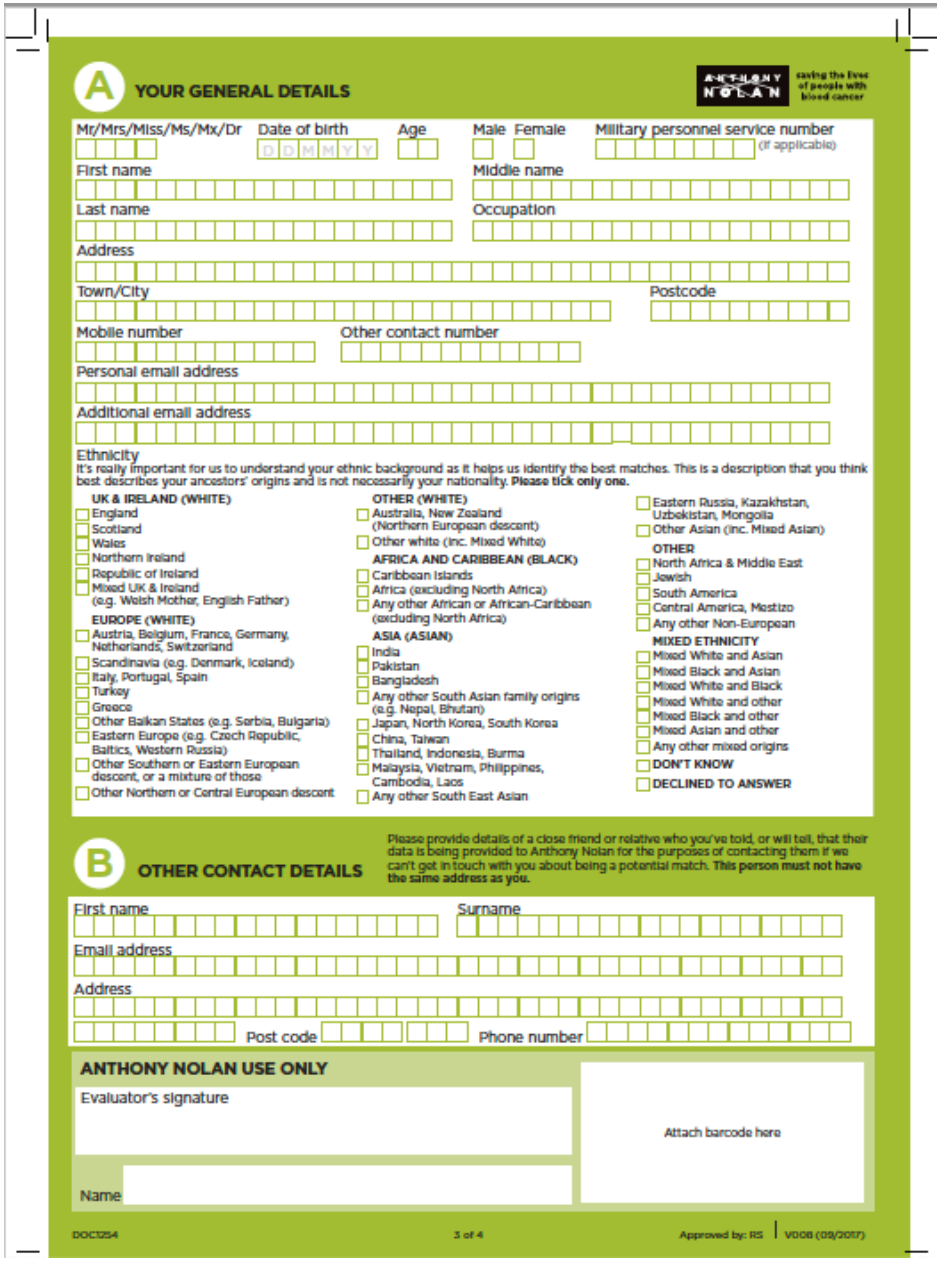
About your data

If you have any questions about data protection or wish to request your personal information, you can contact us at the 'Head Office' address below, or email **dataprotection@anthonynolan.org**. If you have a complaint about how we have handled your personal information, you can contact us and we will investigate.

*'UK', 'our' or 'we' refers to the registered charity Anthony Nolan (no. 803716 in England and Wales/ no. SC038927 in Scotland) and a company limited by guarantee (company no. 02379280) and Anthony Nolan Trading Limited, a limited company (company no. 02579952).

Registered address: The Royal Free Hospital, Pond Street, Hampstead, London, NW3 2QG
Head Office: 2-3 Heathgate Place, 75-87 Agincourt Road, NW3 2NU

**We are registered with the UK Information Commissioner's Office (ICO) as a data controller under registration number Z3022117 (Anthony Nolan) and Z4877402 (Anthony Nolan Trading Limited).



A YOUR GENERAL DETAILS

ANTHONY NOLAN saving the lives of people with blood cancer

Mr/Mrs/Miss/Ms/Mx/Dr | Date of birth (D D M M Y Y) | Age | Male | Female | Military personnel service number (if applicable)

First name | Middle name

Last name | Occupation

Address

Town/City | Postcode

Mobile number | Other contact number

Personal email address

Additional email address

Ethnicity

It's really important for us to understand your ethnic background as it helps us identify the best matches. This is a description that you think best describes your ancestors' origins and is not necessarily your nationality. **Please tick only one.**

UK & IRELAND (WHITE)
- England
- Scotland
- Wales
- Northern Ireland
- Republic of Ireland
- Mixed UK & Ireland (e.g. Welsh Mother, English Father)

EUROPE (WHITE)
- Austria, Belgium, France, Germany, Netherlands, Switzerland
- Scandinavia (e.g. Denmark, Iceland)
- Italy, Portugal, Spain
- Turkey
- Greece
- Other Balkan States (e.g. Serbia, Bulgaria)
- Eastern Europe (e.g. Czech Republic, Baltics, Western Russia)
- Other Southern or Eastern European descent, or a mixture of those
- Other Northern or Central European descent

OTHER (WHITE)
- Australia, New Zealand (Northern European descent)
- Other white (inc. Mixed White)

AFRICA AND CARIBBEAN (BLACK)
- Caribbean Islands
- Africa (excluding North Africa)
- Any other African or African-Caribbean (excluding North Africa)

ASIA (ASIAN)
- India
- Pakistan
- Bangladesh
- Any other South Asian family origins (e.g. Nepal, Bhutan)
- Japan, North Korea, South Korea
- China, Taiwan
- Thailand, Indonesia, Burma
- Malaysia, Vietnam, Philippines, Cambodia, Laos
- Any other South East Asian
- Eastern Russia, Kazakhstan, Uzbekistan, Mongolia
- Other Asian (inc. Mixed Asian)

OTHER
- North Africa & Middle East
- Jewish
- South America
- Central America, Mestizo
- Any other Non-European

MIXED ETHNICITY
- Mixed White and Asian
- Mixed Black and Asian
- Mixed White and Black
- Mixed White and other
- Mixed Black and other
- Mixed Asian and other
- Any other mixed origins

- **DON'T KNOW**
- **DECLINED TO ANSWER**

B OTHER CONTACT DETAILS

Please provide details of a close friend or relative who you've told, or will tell, that their data is being provided to Anthony Nolan for the purposes of contacting them if we can't get in touch with you about being a potential match. **This person must not have the same address as you.**

First name | Surname

Email address

Address

Post code | Phone number

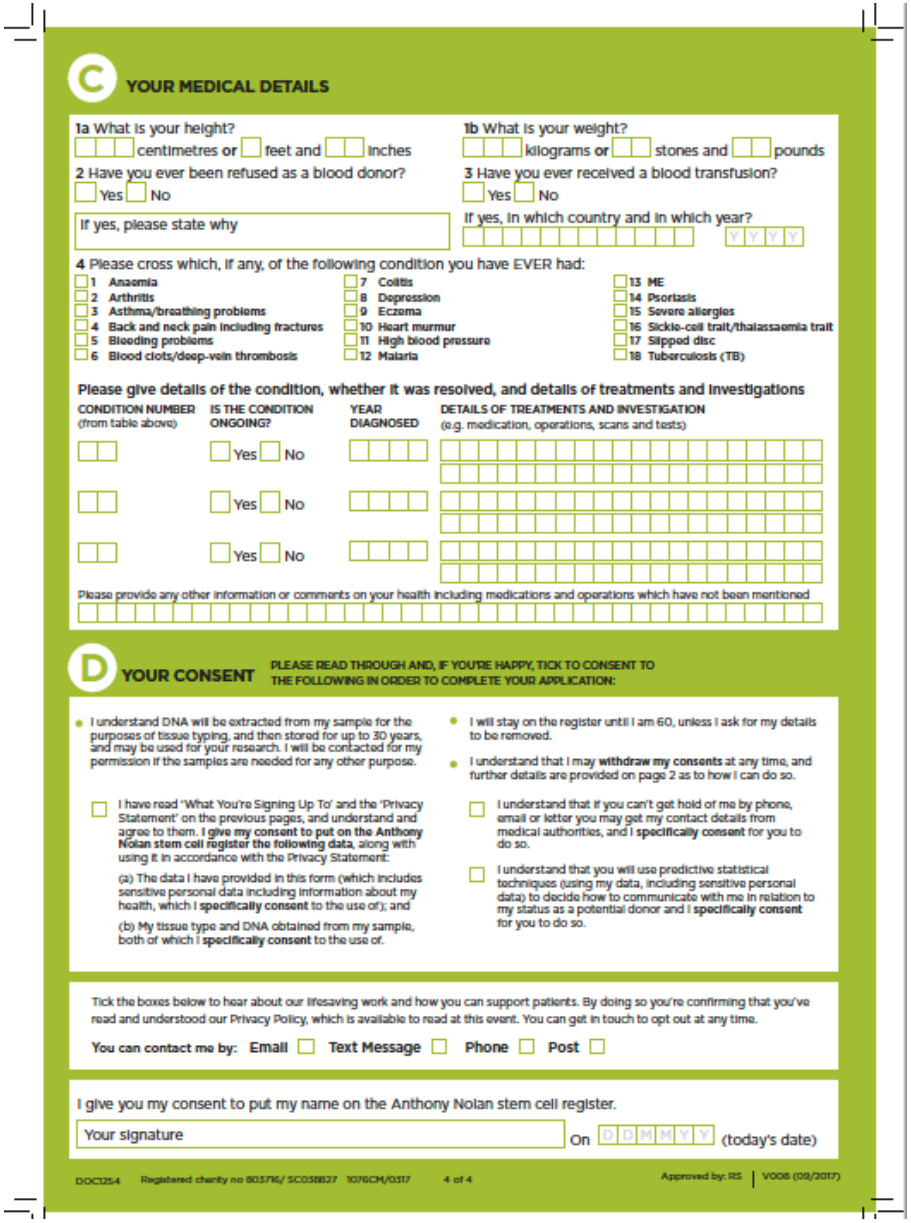
ANTHONY NOLAN USE ONLY

Evaluator's signature

Attach barcode here

Name

DOC1254 | 3 of 4 | Approved by: RS | V008 (09/2017)



C YOUR MEDICAL DETAILS

1a What is your height?
☐☐☐ centimetres **or** ☐ feet and ☐☐ inches

1b What is your weight?
☐☐☐ kilograms **or** ☐☐ stones and ☐☐ pounds

2 Have you ever been refused as a blood donor?
☐ Yes ☐ No

If yes, please state why

3 Have you ever received a blood transfusion?
☐ Yes ☐ No

If yes, in which country and in which year?
☐☐☐☐☐☐☐☐☐☐☐☐ Y Y Y Y

4 Please cross which, if any, of the following condition you have EVER had:

- ☐ 1 Anaemia
- ☐ 2 Arthritis
- ☐ 3 Asthma/breathing problems
- ☐ 4 Back and neck pain including fractures
- ☐ 5 Bleeding problems
- ☐ 6 Blood clots/deep-vein thrombosis
- ☐ 7 Colitis
- ☐ 8 Depression
- ☐ 9 Eczema
- ☐ 10 Heart murmur
- ☐ 11 High blood pressure
- ☐ 12 Malaria
- ☐ 13 ME
- ☐ 14 Psoriasis
- ☐ 15 Severe allergies
- ☐ 16 Sickle-cell trait/thalassaemia trait
- ☐ 17 Slipped disc
- ☐ 18 Tuberculosis (TB)

Please give details of the condition, whether it was resolved, and details of treatments and investigations

CONDITION NUMBER (from table above)	IS THE CONDITION ONGOING?	YEAR DIAGNOSED	DETAILS OF TREATMENTS AND INVESTIGATION (e.g. medication, operations, scans and tests)
☐☐	☐ Yes ☐ No	☐☐☐☐	
☐☐	☐ Yes ☐ No	☐☐☐☐	
☐☐	☐ Yes ☐ No	☐☐☐☐	

Please provide any other information or comments on your health including medications and operations which have not been mentioned

D YOUR CONSENT

PLEASE READ THROUGH AND, IF YOU'RE HAPPY, TICK TO CONSENT TO THE FOLLOWING IN ORDER TO COMPLETE YOUR APPLICATION:

- I understand DNA will be extracted from my sample for the purposes of tissue typing, and then stored for up to 30 years, and may be used for your research. I will be contacted for my permission if the samples are needed for any other purpose.
- I will stay on the register until I am 60, unless I ask for my details to be removed.
- I understand that I may **withdraw my consents** at any time, and further details are provided on page 2 as to how I can do so.

☐ I have read 'What You're Signing Up To' and the 'Privacy Statement' on the previous pages, and understand and agree to them. **I give my consent to put on the Anthony Nolan stem cell register the following data**, along with using it in accordance with the Privacy Statement:

(a) The data I have provided in this form (which includes sensitive personal data including information about my health, which I **specifically consent** to the use of); and

(b) My tissue type and DNA obtained from my sample, both of which I **specifically consent** to the use of.

☐ I understand that if you can't get hold of me by phone, email or letter you may get my contact details from medical authorities, and I **specifically consent** for you to do so.

☐ I understand that you will use predictive statistical techniques (using my data, including sensitive personal data) to decide how to communicate with me in relation to my status as a potential donor and I **specifically consent** for you to do so.

Tick the boxes below to hear about our lifesaving work and how you can support patients. By doing so you're confirming that you've read and understood our Privacy Policy, which is available to read at this event. You can get in touch to opt out at any time.

You can contact me by: Email ☐ Text Message ☐ Phone ☐ Post ☐

I give you my consent to put my name on the Anthony Nolan stem cell register.

Your signature On D D M M Y Y (today's date)

GDPR ready website privacy policy for donors: https://www.anthonynolan.org/privacy-policy

Explanation provided by WMDA

matching donors • serving patients

Explanatory information on Data Use Agreements (DUAs) for organisations listing donors/cord blood products in the global Search & Match Service

NOTE: This explanation is focused on the European Union (EU) privacy obligations in establishing inter-organisational privacy agreements (i.e., Data Use Agreements (DUA)). However, while this information emphasizes specific EU requirements and expectations, the need for a similar agreement is common across most international legal jurisdictions.

The EU privacy regulation (GDPR) is more verbose on the contractual terms of the DUA, compared with other similar international regulations. As WMDA processes data on behalf of many global organisations and is domiciled in the European Economic Area, WMDA has chosen to align its DUA to comply with GDPR to ensure an acceptable global standard for all of its members.

EXECUTIVE SUMMARY

A new EU privacy law, the General Data Protection Regulation (GDPR), is set to replace the prior EU Data Protection Directive 95/46/ec, effective May 25, 2018. GDPR establishes a harmonized set of privacy obligations for the "processing" (performance of any "operation" on personal data, for example, collection, organisation, storage, alteration, or use) of the personal data of European residents. With regard to third party data processing of personal data, GDPR expands significantly upon an organisation's responsibility for overseeing its third-party processing activities and sets out specific rules for allocating responsibility between the organization and its third-party data processors. All WMDA member organisations that collect or process European personal data will likely need to take action.

GDPR Article 28 requires that organisations must only use third party processors that can provide "sufficient guarantees" in ensuring the protection of the privacy and rights of the data subject. The processing directives between the organisation and its third-party processors must be governed by a binding contract. These contracts must direct and control the purpose of processing, onward sharing of data, data subject rights, and other privacy and security obligations, to allow the controller's purpose to be achieved while also protecting the privacy rights and freedoms of the data subject. This contract between an organisation and its third-party processors is commonly called a Data Use Agreement (DUA). The DUA must be in place and executed directly between two legal entities sharing European personal data. As noted above, most countries have a similar principle in their respective privacy regulations.

International organisations listing donors/cord blood products have, at a minimum, two primary data sharing arrangements that must be governed by the DUA described above. First, any organisation listing its donors and/or cord blood units with WMDA, or receiving personal data via WMDA, will need to execute a Listing organisation-WMDA DUA. Further, any registry that is sharing or receiving personal data directly from another registry, outside of WMDA, will likely require a Registry-Registry DUA. A template of a Registry-Registry DUA is available for WMDA members through WMDA Share. These WMDA-issued DUAs have been reviewed and approved

An association of members who share a passion for donor care and strive to find the

matching donors • serving patients

by legal counsel and determined to contain the necessary information to comply with the DUA obligations of GDPR. Some organisations may also be using sub-processors (e.g., IT service providers) as part of their operations to process European personal data. As the sub-processing arrangements require similar guarantees and legal agreements, registries may feel compelled to inventory any sub-processing and reassess their vendor agreements to achieve compliance.

INTERNATIONAL TRANSFERS OF PERSONAL DATA

In general, European personal data can be transferred to a third country only if certain conditions are met by both the controller and processor. These conditions include: the third country has achieved an "adequacy" designation (Art. 45); the organisation has taken upon themselves to provide "appropriate safeguards" (Art. 46); or the data subject has explicitly consented to the proposed transfer, after having been informed of the possible risks (Art. 49.1.a). As of this writing, the European Commission has so far recognized Andorra, Argentina, Canada (commercial organisations), Faroe Islands, Guernsey, Israel, Isle of Man, Jersey, New Zealand, Switzerland, Uruguay and the US (limited to the Privacy Shield framework) as providing adequate protection.

As many WMDA organisations are not in a country with an adequacy designation, the DUA templates provided by WMDA rely either on consent, or on the declaration of appropriate safeguards – specifically through a set of Standard Contractual Clauses preapproved by the European Commission. These terms allow for the lawful export of European personal data in the scenarios where the third-countries do not have an adequacy designation.

NEXT STEPS

Today, you received a copy of the Data Use Agreement between WMDA and the listing entities together with this information. You do not have to sign this copy. Next week, we will send out the official Data Use Agreement by using DocuSign to collect your signature.

ADDITIONAL QUESTIONS

In case you have questions about the data use agreement, you can consult the members of the Data Security Privacy Committee during the IDRC in Munich. You can ask for advice from 9-10:00 AM at the 27th of June in room 'Singapore'. Additional questions can also be send by email to jorine.koenderman@wmda.info.

Disclaimer: This information and the commentary contained in it are not legal advice. GDPR is a complex principle-based law which is open to interpretation and also contains numerous areas where Member States are permitted to include additional requirements to the core GDPR requirements. There is currently very limited guidance and commentary on Article 28 GDPR, and supervisory authorities and courts may take different views to those expressed here. GDPR also creates significant compliance risk introducing fines of up to 4% of annual worldwide turnover for the most serious breaches, as well as the risk of private claims by data subjects for compensation. It is strongly recommended that organisations seek legal advice on how to prepare for GDPR, including in relation to the contractual relationships between data processors and data controllers.

An association of members who share a passion for donor care and strive to find the

WISP Australian Registry

ABMDR
Australian Bone Marrow Donor Registry

INFORMATION SECURITY POLICY

Document Authoriser

1. Purpose

The Australian Bone Marrow Registry (ABMDR) operates in a highly regulated environment, and all staff must comply with legislation and applicable polices as determined by:

- the Privacy Act 1988 (Privacy Act) and the Australian Privacy Principles (APPs)
- EU General Data Protection Regulation 2016
- other applicable Acts.

The Information Security Policy (this document) defines the controls to allow the ABMDR to:

- protect information from threats, whether internal or external, deliberate or accidental
- ensure all personnel are clear about their roles and responsibilities in using and protecting information
- effectively manage risks and implement proportionate controls
- protect the organisation from inappropriate use of information.

The ABMDR has adopted the international standard ISO 27001- Information Security Management as its guide for managing information security risks across the organisation.

2. Scope

The policy applies to:

- all of ABMDR
- partners, suppliers, and service providers of information and technology assets to the divisions; and
- external companies and organisations that the ABMDR divisions provide services to and receive services from.

Employees should understand that a breach to this policy may lead to disciplinary action, which may include termination of employment. In addition, if an employee breaks the law they may also be personally liable for their action.

ICT Information Management and Security Policy

1 Purpose

To ensure that Information Security measures are in place, commensurate with their Information Asset classification, to protect Information Assets, Information and Communication Technology (ICT) Assets and Information Systems within the University ICT environment against unauthorised use or accidental modification, loss or release; and assist the University mitigate any damage or liability arising from the use of these Information Assets and Information Systems for purposes contrary to the University's policies and relevant Regulatory Compliance Instrument.

2 Scope

This policy applies to all Employees, Research Workers, University Members and Students (hereafter referred to as 'users') who have access to the University's Information Assets and related Information Systems.

Example of NMDP

Example of ZKRD