

Introduction

Rural Doctors Workforce Agency (RDWA) collects, uses and stores personal information necessary for the functions of the organisation.

The range of functions that RDWA carries out includes those related to:

- the delivery of services for the rural workforce, including locum medical services in rural practices, the recruitment of Australian and international health professionals, professional development activities, the provision of grants, scholarships and incentive payments, support services and payments for health professionals who provide visiting services, personal support and awareness raising programs for the current and for the future health workforce, workforce planning, workforce research, maintaining accurate data on the rural primary health workforce and the practices in which health professionals work, business support services for rural practices, and
- managing the affairs of the organisation, including handling complaints, running our website, sending newsletters to subscribers, and reporting to agencies such as the Australian Charities and Not for Profit Commission, the Australian Taxation Office and the Child Support Agency.

RDWA is required to meet the obligations of the *Privacy Act 1988* (the Act) including the Australian Privacy Principles (APP) defined by the Act.

RDWA is also required to comply with the *General Data Protection Regulation (EU) 2016/679* (GDPR) (<https://eugdpr.org/>) where the RDWA collects personal information of residents of the European Union. For the purpose of the GDPR, RDWA is a data controller.

Definitions

'Information' or a 'record' are information in electronic or hard copy form. It includes pictures and databases but does not relate to information or records that are publicly available or to employee records which are exempted by the Act.

'Personal information' is information that identifies an individual, and the person does not have to be mentioned by name for information to be considered personal information. A record or information will contain personal information if an individual can be 'reasonably identified' from the record or information.

'Sensitive information' is personal information relating to an individual's:

- racial or ethnic origin, including country of birth;
- political opinions;
- membership of a political association;
- religious beliefs or affiliations;
- philosophical beliefs;
- membership of a professional or trade association;
- membership of a trade union;
- sexual orientation or practices;
- criminal record;
- child related employment screening reports;
- health;
- genetics; and
- biometrics.

For the GDPR, sensitive information is also be referred to as 'special category data' in this policy.

'Data controller' for the purposes of the GDPR is the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal information.

'Data processor' for the purposes of the GDPR means a natural or legal person, public authority, agency or other body which 'processes' personal data on behalf of a data controller, and in accordance with the data controller's instructions.

'Data subject' for the purposes of the GDPR is an individual who is physically located in the European Union at the time that their personal information is collected by RDWA. A person does not need to be a citizen of a European country in order to be considered a data subject.

'Member State' for the purposes of the GDPR is any one of the member states of the European Union.

Policy Statement

RDWA is committed to:

- protecting an individual's right to privacy in relation to the collection, management, storage, use and disclosure of personal information; and
- ensuring the accuracy and security of any personal information it holds in relation to individual regardless of whether those individuals are staff, service users, contractors or visitors.

RDWA will only collect and retain personal information if it is reasonably necessary for the services and activities of the organisation, where it is able to do so in a lawful way, and if it is required to do so by law.

It is necessary for RDWA to collect personal and sensitive information in physical records and electronic files. RDWA does this in a number of ways, including:

- directly from individuals through email, telephone and when the individual completes a form;
- from third parties such as government departments; and
- through marketing events.

RDWA will deal with unsolicited personal or sensitive information in accordance with the APP, which generally means that the information will be destroyed or de-identified where it is reasonable to do so.

Scope

This policy applies to the whole of RDWA. It is a general policy which deals with the broad privacy practices of the organisation and may be changed from time to time as information handling practices change. Users should check this policy on a regular basis. Each time the Policy is updated, the date of the change will be stated on the policy, so users will be able to determine if there have been changes since the policy was read previously.

Collection of Personal and Sensitive Information

With the range of services provided by RDWA, there is a significant amount of personal information collected. Personal information collected by RDWA can include:

- Name, gender and date of birth
- Photographs
- Emergency contact details
- Email addresses
- Residential and postal addresses and telephone numbers
- Business, position and contact details
- Grant application forms and supporting documentation including residency status, health practitioner registration and employment details

- Information received as part of a recruitment process and supporting documentation including health practitioner registration details, residency status and passport and visa details;
- Application forms for government programs for which RDWA is a government delegate, and supporting information
- Government related identifiers such as tax file numbers.

A person has the right to refuse to provide personal information to RDWA, however that may affect RDWA's ability to meet its obligations to that person or to a third party such as a government agency.

RDWA will only seek and collect sensitive information if it is required to do so by law or if it has the consent of the individual and it is reasonably necessary to have this information for the RDWA to carry out the relevant function or activity.

Notification of the Collection of Personal Information

Prior to or at the time that RDWA collects personal information, RDWA will take reasonable steps to notify the person of the purpose as to why RDWA needs to collect the information, contact details for RDWA and that the information has been collected.

Use and Disclosure of Personal Information

Use of Personal Information

RDWA collects personal information on the lawful basis that it is necessary to perform its obligations to:

- individuals under a contract with that individual
- performing a task for RDWA's legitimate interests, including
 - communicating to users about the services or grants that are offered by RDWA;
 - in general financial management of the organisation;
 - to collate information for review of programs and services it provides to users; or
 - to collate contact details for employees, service users, visitors and business stakeholders.

Disclosure of Personal Information

RDWA's primary reasons for disclosing personal information include:

- to identify an individual
- to provide RDWA services to an individual
- to communicate with an individual.

RDWA will take reasonable steps to ensure that personal information is not disclosed to a third party, except in permitted situations which might include where RDWA has the individual's consent, where it is necessary to provide the information to a third party who provides services to RDWA, or where disclosure is required by law or regulatory obligations such as the Australian Taxation Office.

Where RDWA does provide personal information to a third party within Australia, RDWA will take reasonable steps to ensure the third party is compliant with APP2.

Third parties outside of Australia to whom RDWA may disclose personal information include information technology service providers, including cloud service providers.

The Act permits use or disclosure of information without an individual's consent where it may be necessary to prevent a serious and imminent threat to any person's life, health or safety or a serious threat to public health or safety.

Use of Special Category Data

For the purposes of the GDPR, RDWA will only process special category data of data subjects where:

- a. the data subject has given explicit consent to the processing of those personal data for one or more specified purposes;
- b. processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law in so far as it is authorised by European Union or Member State law or a collective agreement pursuant to Member State law providing for appropriate safeguards for the fundamental rights and the interests of the data subject;
- c. processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent;
- d. processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade union aim and on condition that the processing relates solely to the members or to former members of the body or to persons who have regular contact with it in connection with its purposes and that the personal data are not disclosed outside that body without the consent of the data subjects;
- e. processing relates to personal data which are manifestly made public by the data subject;
- f. processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity;
- g. processing is necessary for reasons of substantial public interest, on the basis of European Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject;
- h. processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of European Union or Member State law or pursuant to contract with a health professional and subject to the conditions and safeguards referred to in paragraph 3;
- i. processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, on the basis of European Union or Member State law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject, in particular professional secrecy;
- j. processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) based on European Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.

Direct Marketing

RDWA does on occasion and where reasonable, use personal information in direct marketing. Direct marketing may occur by mail, email or telephone.

RDWA provides a simple and readily identifiable means for an individual to refuse to receive direct marketing, and by which the individual may opt out from receiving marketing to which they had previously consented to receiving.

Cross -border Disclosure of Personal Information

The scope of RDWA's functions includes international activity related to recruitment of internationally qualified health professionals and/or health professionals located outside of Australia, and RDWA may transmit personal information in the conduct of these functions overseas. The countries in which such recipients are likely to be located include, but are not limited to, the United States, the United Kingdom, Ireland, India, Sri Lanka, Pakistan, Malaysia and Singapore.

If it is necessary to disclose personal information overseas, the actual consent of the individual will, wherever practicable, be sought before the information is disclosed.

If it is not reasonably practicable to obtain the consent of the individual concerned, RDWA will only transmit the personal information where it must do so according to a relevant law.

Where RDWA uses marketing and survey services provided by third parties offshore such as Google and Facebook, the disclosure of personal information will be for the purpose of marketing RDWA's services to users, and individuals will be provided a simple means of opting out of the marketing communications.

Security of Personal Information

RDWA will take all reasonable steps to ensure the personal information it collects, uses or discloses is accurate, up to date, complete and relevant, and has regard for the purpose of the collection, use or disclosure.

RDWA expects that individuals providing personal information to RDWA ensure that the personal information they provide is relevant and accurate.

RDWA will take reasonable steps to protect personal information it holds from:

- misuse, interference and loss; and/or
- unauthorised access, modification or disclosure.

RDWA has in place computer software and hardware that provides electronic protection of and/or prevents access to personal information from unauthorised persons, particularly from those individuals who are external to RDWA.

Electronic protection includes mitigation strategies to prevent unauthorised access, prevent malware delivery and execution, limit the extent of cyber security incidents and ensure recovery of data and system availability:

- mandatory password protection on computers
- restricted administrative privileges to operating systems and applications including multi-factor authentication
- latest version operating systems
- Microsoft Office Macros are disabled and security settings cannot be changed by users
- Layer 7 Firewall rules and content filtering
- Antivirus software
- email threat protection software.

Generally, subject to an individual's right to erasure, personal information retained by RDWA will be stored for as long as RDWA requires it to carry out the purpose for which the data was collected, following which time it will be either destroyed or de-identified.

Access to Personal Information

RDWA will manage requests for access or correction by an individual of their personal information held by RDWA in accordance with this policy.

All requests must be made in writing and in appropriate form as defined by RDWA from time to time. On receipt of an application and within a reasonable timeframe RDWA will take reasonable steps to inform the individual who made the request:

- what personal information RDWA holds in relation to that individual;
- why the personal information is held;
- how RDWA collects (or collected), holds (or held), uses (or used) and discloses (or disclosed) the personal information.

RDWA will confirm with the individual whether they wish to have access to the personal information in question, and RDWA will ordinarily give an individual access to their personal information unless an exception applies.

Exceptions include where:

- giving access would have an unreasonable impact on the privacy of other individuals;
- the request for access is frivolous or vexatious;
- the request is manifestly unfounded or excessive (taking into account whether the request is repetitive in nature); or
- the access would be unlawful.

RDWA will not charge for making an access or correction request.

If a request for access or correction is denied by RDWA it will, within a reasonable time period, provide the individual who made the request with a general, written explanation as to why the request was refused.

Accuracy and Correction of Personal Information

RDWA will be obliged, without an individual's request for correction, to correct inaccurate, out-of-date, incomplete, irrelevant or misleading personal information if RDWA is satisfied that, having regard to the purpose for which the personal information is held, the information is inaccurate, out-of-date, incomplete, irrelevant or misleading.

If this occurs, RDWA must take all reasonable steps to correct that information to ensure that, having regard to the purpose for which it is held, the information is accurate, up-to-date, complete, relevant and not misleading.

If an individual is of the view that their personal information requires correction, they should contact the Privacy Officer listed below.

Data Breaches

In accordance with the National Data Breach (NDB) Scheme, in the event of a suspected data breach RDWA will:

- contain the breach and, if possible, take remedial action; and
- commence the assessment process to determine whether the data breach is likely to be an 'eligible data breach' for the purposes of the NDB Scheme.
- An 'eligible data breach' is where:
 - there is unauthorised access to, unauthorised disclosure of, or loss of, personal information held by it;
 - the access, disclosure or loss is likely to result in 'serious harm' to any of the individuals to whom the information relates. In this context, 'serious harm' refers to serious physical, psychological, emotional, financial or reputational harm to an individual or individuals; and
 - RDWA has not been able to prevent the likely risk of serious harm with remedial action.

If RDWA reasonably believes that an 'eligible data breach' has occurred, it will:

- prepare a statement to the Office of the Australian Information Commissioner (OAIC) as soon as practicable (OAIC Statement);
- notify the individual to whom the information relates as soon as practicable after the statement has been prepared.

Obligations under the GDPR

In accordance with the GDPR, RDWA will ensure that:

- on becoming aware of a data breach,:
 - it will attempt to contain it and assess the potential adverse consequences for individuals involved; and
- if, after conducting an assessment, it considers that there is a risk to an individual's rights and freedoms as a result of the personal data breach,
 - it will report the breach to the relevant Supervisory Authority without undue delay and, where feasible, not later than 72 hours after becoming aware of the breach; and
- If there is a high risk to an individual's rights and freedoms as a result of the personal data breach,
 - it will report the breach to the relevant Supervisory Authority in accordance with the clause above and notify the individual affected without undue delay.

RDWA will keep a record of all personal data breaches, regardless of whether or not they need to be reported to the Supervisory Authority.

RDWA will not report a personal data breach in the event that, after conducting an assessment, RDWA considers that the risk of harm to an individual's rights and freedoms is unlikely.

A 'personal data breach' for the purposes of the GDPR includes, but is not limited to, whenever any personal data is lost, destroyed, corrupted or disclosed; if someone accesses the data or passes it on without proper authorisation; or if the data is made unavailable, for example, when it has been encrypted by ransomware, or accidentally lost or destroyed.

Additional Rights of European Residents Under The GDPR

European Residents have a number of additional rights under the GDPR in addition to the protections afforded under the Act and the APPs, including:

- the right to receive personal data you have provided to RDWA in a structured, commonly used and machine-readable format, including the right to request that RDWA transmits this data directly to another data controller;
- the right to restrict the processing of your personal data in certain circumstances. This means that you can limit the way that RDWA uses your data (this right is an alternative to requesting the erasure of your data); and
- the right to require RDWA to erase your data in certain circumstances.

Contracts with Third Party Data Processors

In the event that RDWA engages a data processor to process the personal data of European Residents on RDWA's behalf, it will only do so if that data processor has provided RDWA with sufficient guarantees that it will implement appropriate technical, contractual and organisational measures that ensure compliance with the GDPR, and the protection of the personal information of European Residents.

To the extent that RDWA engages a third-party data processor, it will ensure that it enters into a written agreement with that data processor, which sets out, as a minimum, terms which require the processor to:

- only act on the written instructions of RDWA as the data controller;
- ensure that people processing the data are subject to a duty of confidence;
- take appropriate measures to ensure the security of processing;
- only engage sub-processors with the prior consent of RDWA and under a written contract;
- assist the controller in providing subject access and allowing data subjects to exercise their rights under the GDPR;
- assist RDWA in meeting its GDPR obligations in relation to the security of processing, the notification of personal data breaches and data protection impact assessments;
- delete or return all personal data to RDWA as requested at the end of the contract; and
- submit to audits and inspections, provide RDWA with whatever information it needs to ensure that they are both meeting their Article 28 obligations, and tell RDWA immediately if it is asked to do something infringing the GDPR or other data protection law of the EU or a member state.

Cookies

RDWA uses cookies on its website. Cookies are placed on your computer or mobile device when you visit a website to ensure website functionality, track usage patterns, personalise content and advertisements, analyse traffic and to enable social media features.

Essential cookies are those necessary for the website to function, and essential cookies do not generally collect personal information. Non-essential cookies may collect personal information.

The cookies used by RDWA may be set by RDWA itself, or by third parties. RDWA uses the following non-essential cookies (some of which are set by third parties), for the following identified purposes:

- Facebook
- Google (for ad retargeting)
- Google Analytics (reporting)

You have the right to decide whether to accept or block cookies; however if all cookies are blocked the functionality of our website may be impaired.

You can control your cookie preferences by adjusting your browser settings. Most browsers automatically accept cookies, therefore if you do not wish cookies to be used you may need to actively delete or block cookies.

To the extent that any cookies placed on RDWA's website by RDWA or a third party can uniquely identify a European Resident, the requirements of the GDPR will be adhered to.

In particular, RDWA will ensure that:

- consent is obtained prior to the setting of the cookies
- consent to the use of cookies can be provided by clear affirmative, positive action;
- rejecting the use of cookies will be an actual option in the sense that a European Resident can continue to access our website and its functions even if all but the essential cookies have been rejected
- a European Resident can withdraw their consent at any time by changing the relevant settings;
- a European Resident's consent is renewed every 12 months;
- it documents a European Resident's consent and stores it securely; and
- it deletes the personal information of a European Resident upon request.

Complaints and Additional Information

If an individual has any questions or concerns, or believes RDWA has breached its obligations under the APP or this policy generally, please contact our Privacy Officer, General Manager, by email at generalmanager@ruraldoc.com.au or by mail to:

Privacy Officer
63 Henley Beach Road
Mile End SA 5031
Phone +61 8 8234 8277

If you are a European Resident and have any questions about RDWA's compliance with the GDPR, please contact the Privacy Officer, RDWA General Manager (who is also RDWA's Data Protection Officer for the purposes of the GDPR) in the first instance.