**Policy name** Privacy
**Author** Emma Spiers, National Manager, UK
**Approved by** Natalie Keating, Chief Executive Officer, UK

## 1. Rationale and Purpose

The Better Health Generation is committed to ensuring that the delivery of all services is compliant with associated and required legislative obligations. The purpose of this policy is to establish The Better Health Generation's intent with regard to the, Privacy Amendment (Enhancing Privacy Protection) Act 2012 (Cth) and the Privacy Act 1988 (Cth), incorporating the 13 Australian Privacy Principles, Privacy Amendment (Notifiable Data Breaches) Act 2017 (Cth), as well as the following state legislations:

- Privacy and Personal Information Protect Act 1998 (NSW)
- Health Records and Information Privacy Act 2002 (NSW).
- Health Records Act 2001 (VIC).
- Privacy and Data Protection Act 2014 (VIC).
- Personal Information and Protection Act 20014 (TAS).
- Information Privacy Act 2009 (QLD).
- Health Records (Privacy and Access) Act 1997 (ACT).
- Information Privacy Act 2014 (ACT).
- Health Care Act 2008 (SA).
- Information Act 2003 (NT).

## 2. Scope of Policy

This policy applies to all The Better Health Generation team members, contractors and service providers.
**Please note:** The Better Health Generation means The Better Health Generation and all of its subsidiaries.

### RESPONSIBILITIES

The following responsibilities are established for maintaining and safeguarding the privacy of all personal information:

#### Chief Executive Officer

The Chief Executive Officer of The Better Health Generation is responsible for:

**Policy name** Privacy
**Author** Emma Spiers, National Manager, UK
**Approved by** Natalie Keating, Chief Executive Officer, UK

- Ensuring sufficient resources are in place to ensure The Better Health Generation meets its legislative obligations, and ensure the effectiveness and currency of all policies, procedures and task guides in relation to the protection of privacy of personal information.
- Ensuring processes and resources are in place to act accordingly where possible breaches of privacy are evident, in upholding this policy.
- Approval of this policy, and any subsequent policy reviews or amendments.
- Upholding the requirements of this policy where relevant, for any Executive Leadership Team decisions or actions.

**Quality Management Systems Manager:**

QMS Manager is responsible for;

- Ensuring the effectiveness and currency of the privacy policy, as well as ensuring adequate processes are established to maintain compliance with the obligations of the legislation, including any staff training resources.
- Monitoring systems that relate to the privacy of personal information, and ensuring cyclical tasks associated with privacy compliance are undertaken on time and when due, including annual staff refresher training and cyclical destruction of personal information (including electronic information).

## Management Staff

Management staff (i.e. any staff member with management responsibilities) are responsible for ensuring staff under their scope of management are:

- Adequately trained in The Better Health Generation's privacy processes.
- Competent in implementing and complying with our privacy obligations.
- Successful in completing privacy training during induction and then at least annually.
- Compliant in service delivery and other tasks and activities, to ensure privacy is guaranteed.
- Managed accordingly and promptly, and in accordance with this policy, should breaches of privacy occur

## All Staff

All staff are responsible for:

**Policy name** Privacy
**Author** Emma Spiers, National Manager, UK
**Approved by** Natalie Keating, Chief Executive Officer, UK

- Complying with the obligations of privacy legislation and acting responsibly and ethically in all matters pertaining to privacy.
- Implementing procedures and task guides in a compliant manner to ensure that privacy obligations are met.

## GUIDING PRINCIPLES AND DESIRED OUTCOMES

- The Better Health Generation is committed to maintaining and safeguarding the privacy of all individual's personal information, including sensitive information. As such, The Better Health Generation will:
- Document and implement procedures and task guides to assist assure the integrity, accuracy, completeness, relevance and currency of records of personal information.
- Only collect personal information that is relevant to service provision or functions and activities of the organisation.
- Store personal and/or sensitive information in a secure area with safeguards in place to minimise loss, unauthorised access and use, modification or misuse, for periods of time that are appropriate with our service delivery requirements, business functions and activities and any additional legislative or contractual obligations.
- Collect and store personal information in a manner that will meet external reporting requirements as well as meet legislative obligations and provide security with respect to maintaining privacy of personal information.
- Limit access to and use of personal information to that which is outlined within this policy.
- Act effectively and efficiently on all matters pertaining to privacy.
- Assist and inform clients and consumers to provide assurance that The Better Health Generation has met its obligations with respect to privacy.
- Undertake cyclical processes to ensure a high level of knowledge is maintained within the organisation to assure privacy of information, and to ensure that retention of personal information meets current legislative requirements.
- Undertake sufficient risk assessment and treatment protocols to ensure personal information is sufficiently protected.
- Act in accordance with the Notifiable Data Breaches scheme

**Policy name** Privacy
**Author** Emma Spiers, National Manager, UK
**Approved by** Natalie Keating, Chief Executive Officer, UK

## 3. Policy

Open and transparent management of personal information

This policy section relates specifically to Australian Privacy Principle 1 – Open and transparent management of personal information.

The Better Health Generation will manage personal information in an open and transparent manner. As such, The Better Health Generation will:

- Collect personal information, including sensitive health information, which is relevant to the service being provided to the client in a manner that is not intrusive or unreasonable. This may include, but is not limited to:
- Personal details including but not limited to name, address, contact information, next of kin and date of birth.
- Medical reports and records including medical certificates, investigation and assessment findings and reports, previous rehabilitation provider or disability services provider records, contact information for current and past health providers, and health providers information from successive health providers to assist with service delivery.
- Personal information from employment service providers and NDIS Support coordinators, including claim/client/case numbers.
- Details pertaining to provision of welfare payments, wage details, or any other financial information or data relating to the service being provided.
- Employment history including but not limited to details of skills, abilities, training undertaken, past and current employer details.
- Personal details including but not limited to name, address and contact information.
- Employment history including but not limited to details of skills, abilities, training undertaken, past and current employer details.
- Copies of qualifications and training records.
- Personal information that may minimise or mitigate business risks that may be inherent in any employment based relationship.
- Any other personal or health related information that is reasonable and necessary in relation to the condition to which The Better Health Generation has been specifically engaged.
- Store all information collected in a manner which ensures its privacy and access by those who are duly authorised.
- Where personal information is stored in an electronic manner The Better Health Generation will ensure sufficient security protocols are in place to ensure access is restricted to those employees

who are involved in the delivery or services, the assurance of quality service delivery, management of service delivery or the administration of service delivery.

- Where personal information is stored in hard copy the personal information will be secured in a lockable environment that ensures restricted access in a manner that is equivalent to that of electronic records.
- Ensure that procedures are in place to establish how an individual may determine if health information is held by us, how they can access their personal information that is held by The Better Health Generation, and seek the correction of such personal information.
- Establish and maintain procedures to accept and act upon complaints regarding breaches of the Australian Privacy Principles, health record legislation, or a registered APP code (if any) that binds The Better Health Generation
- Not release or disclose personal information to overseas recipients unless this has been previously outlined in The Better Health Generation's privacy policy.
- Not charge clients for making a request to access to their personal information held by The Better Health Generation, and provide duplicates of personal information at minimum cost to clients.
- Not charge for the provision of our privacy policy.
- Ensure that a client's needs in relation to the format of our privacy policy are met in all reasonable circumstances.
- Continually collect personal information during the period of service provision to facilitate a quality service delivery.

## Anonymity and pseudonymity

This policy section relates specifically to Australian Privacy Principle 2 – Anonymity and pseudonymity.

Under the Australian Privacy Principles individuals are provided with the option of not identifying themselves, or using a pseudonym when dealing with The Better Health Generation in relation to particular matters. The Better Health Generation will uphold this option wherever practical, and where it is deemed that we are not at risk of being non-compliant with any other Australian Privacy Principle.

In certain circumstances it may be impractical to offer clients the option of not identifying themselves, or using a pseudonym, for example:

- When services are to be provided under a government based scheme or insurance arrangement, such as, but not limited to NDIS, workers compensation, compulsory third party or life insurance.
- When services are to be provided under a government contract where the deed for service provision requires identification of the client prior to commencement of service delivery.

**Policy name** Privacy
**Author** Emma Spiers, National Manager, UK
**Approved by** Natalie Keating, Chief Executive Officer, UK

- When services are medico-legal in nature.

## Collection of solicited personal information

This policy section relates specifically to Australian Privacy Principle 3 – Collection of solicited personal information.

The Better Health Generation will ensure that personal information collected is reasonably necessary for, or directly related to, one or more of The Better Health Generation's functions or activities. The collection of personal information will be carried out by lawful and fair means, following receipt of written consent from the individual to which the personal information to be collected relates, unless a permitted general or health situation exists (as per below*).

Sensitive information collected from individuals will be subject to:

- Written consent from the individual to which the sensitive information to be collected relates, unless a permitted general or health situation exists (see below*).
- Due consideration by the staff member collecting the sensitive information to the relevance and necessity of the sensitive information in relation to the current services being provided.

### *The following are permitted general and health situations:

- Where the staff member believes that the collection is necessary to lessen or prevent a serious threat to life, health or safety of any individual or to public health or safety, and it is unreasonable or impracticable to obtain the individual's consent to the collection.
- Where The Better Health Generation has reason to suspect that unlawful activity or misconduct of a serious nature, that relates to The Better Health Generation's functions or activities has been, is being, or may be engaged in, and the entity reasonably believes that the collection is necessary for the entity to take appropriate action in relation to the matter.
- Where The Better Health Generation reasonably believes that the collection is reasonably necessary to assist any Australian Privacy Principles (APP) entity, body or person to locate a person who has been reported as missing.

## Collection of confidential personal information from third parties (Victoria)

The Better Health Generation will comply with the Health Records Act (2001) Victoria that impacts on our ability to disclose confidential information gained from a third party regarding a person, and the non-disclosure of this information to the person that the information relates to.

| | |
|---|---|
| **Policy name** | Privacy |
| **Author** | Emma Spiers, National Manager, UK |
| **Approved by** | Natalie Keating, Chief Executive Officer, UK |

## Dealing with unsolicited personal information

This policy section relates specifically to Australian Privacy Principle 4 – Dealing with unsolicited personal information.

In circumstances where The Better Health Generation, or any of its staff members, receives personal information which was not solicited, The Better Health Generation, or any of its staff members, will within a reasonable period of time after receiving the personal information, make a satisfactory determination regarding the appropriateness of the personal information being retained in relation to the services being delivered and The Better Health Generation's functions.

Where it is determined that the unsolicited personal information is appropriate to be retained, and meets all requirements of APP3, the personal information will be retained in accordance with the requirements of this policy.

Where it is determined that the unsolicited personal information is not appropriate to be retained and does not meet all requirements of APP3, the personal information will be removed from all electronic records, and all soft and hard copies will be destroyed or de-identified.

## Notification of the collection of personal information

This policy section relates specifically to Australian Privacy Principle 5 – Notification of the collection of personal information.

The Better Health Generation will ensure that individuals are notified of the circumstances in which we will collect personal information through provision of our privacy statement at the commencement of service delivery or at the commencement of any business related relationship.

Where circumstances change in the manner in which The Better Health Generation collects personal information, The Better Health Generation will take reasonable steps to notify clients of this change.

The Better Health Generation will adopt a best practice stance in notifying consumers of our privacy policy, and will provide access to or a copy of our policy or privacy statement to all current consumers, upon finalisation and approval of any change in practice or policy.

## Use or disclosure of personal information

This policy section relates specifically to Australian Privacy Principle 6 – Use or disclosure of personal information.

| | |
|---|---|
| **Policy name** | Privacy |
| **Author** | Emma Spiers, National Manager, UK |
| **Approved by** | Natalie Keating, Chief Executive Officer, UK |

The Better Health Generation will use personal information that has been collected for the purpose of our functions and activities. The Better Health Generation will not, and does not condone, the use or disclosure of personal information that has been collected for any other purpose, unless:

- The individual to which the collected personal information relates to has consented to the use or disclosure of the information; or
- The individual would reasonably expect The Better Health Generation, or any of its staff members, to use or disclose any sensitive information for a secondary purpose that is directly related to the primary purpose; or
- The individual would reasonably expect The Better Health Generation, or any of its staff members to use or disclose any non-sensitive information for a secondary purpose that is related to the primary purpose; or
- The use or disclosure of the personal information is required or authorised by or under an Australian law or a court/tribunal order; or
- Any of the following exceptions exist and the use or disclosure of personal information is reasonably necessary to:

o Assist in locating a missing person.

o Establish, exercise or defend a legal or equitable claim, or

o For the purposes of a confidential alternative dispute resolution; or

o Any other acceptable purpose as outlined in any state legislation relating to health records and privacy; or.

- The Better Health Generation reasonably believes that the use or disclosure of the personal information is reasonably necessary for one or more enforcement related activities conducted by, or on behalf of, an enforcement body.

## Direct Marketing

This policy section relates specifically to Australian Privacy Principle 7 – Direct marketing.

Use or disclosure of personal information (other than sensitive information) for direct marketing purposes

The Better Health Generation will not use or disclose personal information (other than sensitive information) for the purpose of direct marketing, unless:

- The Better Health Generation has collected personal information from the individual and the individual would reasonably expect The Better Health Generation, or one of its staff members, to use or disclose the personal information for direct marketing and;

| | |
|---|---|
| **Policy name** | Privacy |
| **Author** | Emma Spiers, National Manager, UK |
| **Approved by** | Natalie Keating, Chief Executive Officer, UK |

- The Better Health Generation provides a simple means by which the individual may easily request not to receive direct marketing communications from the organisation; and
- The individual has not made such a request to the organisation.

**The Better Health Generation may use or disclose personal information for the purpose of direct marketing where:**

- The Better Health Generation has collected the personal information from the individual and the individual would NOT reasonably expect The Better Health Generation to use or disclose the information for that purpose; or someone other than the individual and;
- The individual has consented to the use or disclosure of the information from that purpose OR it is impractical to obtain that consent and;
- The Better Health Generation provides a simple means by which the individual may easily request not to receive direct marketing communications from the organisation; and
- In each direct marketing communication with the individual The Better Health Generation includes a prominent statement that the individual may request not to receive direct marketing; or The Better Health Generation otherwise draws the individual's attention to the fact that the individual may make such a request; and
- The individual has not made such a request to the organisation.

Use or disclosure of personal information (other than sensitive information) for direct marketing purposes in capacity as a Commonwealth contracted service provider

The Better Health Generation may use or disclose personal information for the purpose of direct marketing where:

- The Better Health Generation is a contracted service provider for a Commonwealth contract; and
- The Better Health Generation collected the personal information for the purpose of meeting (directly or indirectly) an obligation under the contract, and;
- The use or disclosure is necessary to meet (directly or indirectly) such an obligation.

**Use or disclosure of sensitive personal information for direct marketing purposes**

| | |
|---|---|
| **Policy name** | Privacy |
| **Author** | Emma Spiers, National Manager, UK |
| **Approved by** | Natalie Keating, Chief Executive Officer, UK |

The Better Health Generation may use or disclose sensitive information about an individual for the purpose of direct marketing if the individual has consented to the use or disclosure of the sensitive information for that purpose.

### Facilitating direct marketing by other organisations

The Better Health Generation may, at times, facilitate direct marketing by other organisations. Where The Better Health Generation uses or discloses personal information about an individual for the purpose of direct marketing by The Better Health Generation, or by other organisations, the individual may:

- Request not to receive direct marketing communications from The Better Health Generation; and
- Request The Better Health Generation not to use or disclose the personal information for the purpose of facilitating direct marketing by other organisations; and
- Request The Better Health Generation to provide its source of the personal information.

Where a request has been made of The Better Health Generation to provide its source of personal information, The Better Health Generation will provide this information, at no cost to the individual, and within a reasonable timeframe after the request is made, unless it is impracticable or unreasonable to do so.

### Cross-Border Disclosure of Personal Information

This policy section relates specifically to Australian Privacy Principle 8 – Cross border Disclosure of personal information.

The Better Health Generation does not foresee any future circumstances in which personal information about an individual will be disclosed to an overseas recipient. However, in the circumstances where this may occur, The Better Health Generation will take reasonable steps to ensure that the overseas recipient does not breach the Australian Privacy Principles (other than APP 1) in relation to the information unless sub clause 8.1 of the Australian Privacy Principles does not apply, according to the requirements of the Australian Privacy Principles.

### Trans-border Disclosure of Health Information

This policy section relates specifically to NSW Health Privacy Principle 14 – Trans-border Data Flows and data flow to Commonwealth Agencies; and Victoria Health Privacy Principle 9 – Trans-border data flows.

**Policy name** Privacy
**Author** Emma Spiers, National Manager, UK
**Approved by** Natalie Keating, Chief Executive Officer, UK

The Better Health Generation will not transfer health records or information to a person or body who is in a jurisdiction outside of the state of residence of the individual that the person it relates to, unless specifically permitted under the relative state based legislation.

## Adoption, use or disclosure of government related identifiers

This policy section relates specifically to Australian Privacy Principle 9 – Adoption, use or disclosure of government related identifiers.

Adoption of government related identifiers

The Better Health Generation will not adopt as its own identifier, any government related identifier such as ABN or TFN, an identifier assigned by agency, an agency of an agency acting in this capacity, or a contracted service provider for a Commonwealth contract acting in this capacity.

## Use or disclosure of government related identifiers

The Better Health Generation will not use government related identifiers of an individual unless permitted under the Australian Privacy Principles. The Better Health Generation will use government related identifiers under government contracted services where it is necessary to use this identifier for a function or activity.

The Better Health Generation will not disclose government related identifiers of an individual unless permitted under the Australian Privacy Principles.

The Better Health Generation will de-identify all personal information collected to ensure that government related identifiers of an individual are not disclosed.

The following government related identifiers are unnecessary for our functions and activities:

- Medicare Numbers.
- Tax File Numbers.
- Centrelink customer numbers (excluding job seeker identification numbers).
- Passport numbers.
- Drivers licence numbers.

## Use of other identifiers

The Better Health Generation will use identifiers such as workers compensation claim numbers, and will advise clients regarding the use of such identifiers through provision of our privacy statement.

| | |
|---|---|
| **Policy name** | Privacy |
| **Author** | Emma Spiers, National Manager, UK |
| **Approved by** | Natalie Keating, Chief Executive Officer, UK |

## Quality of personal information

This policy section relates specifically to Australian Privacy Principle 10 – Quality of personal information.

The Better Health Generation will take all reasonable steps, if any, to ensure that the personal information collected is accurate, up to date and complete.

The Better Health Generation will take all reasonable steps, if any, to ensure that personal information disclosed or used throughout the course of service delivery is accurate, up to date, complete and relevant.

## Quality of rehabilitation reports containing personal information

It is essential that all personal information used and disclosed by The Better Health Generation staff is of a high quality. This includes ensuring its accuracy, currency, completeness and relevance.

Staff engaged in service provision, due to the nature of their role, have specific responsibilities when dealing with personal information that may be recorded within a client file or communicated to other stakeholders. This includes:

- Ensuring that the personal information is correct both in its message and in its content.
- Ensuring that the personal information collected and communicated is as up to date as possible and relies on most recent sources of information.
- Ensuring that the personal information is completed in full to ensure the entire scope of the information is clearly communicated.
- Ensuring that any personal information collected and communicated is relevant to our functions and activities in relation to the client to whom the information relates to.

In order to fulfil these responsibilities, it is essential that service delivery staff incorporate the following into their daily activities:

- Ensure that written communication accurately reflects personal information that is collected. This may include ensuring that opinions are distinguished from fact; that sources of personal information are clear (including subjectivity or objectivity) and that sentences are clear and concise.
- That personal information is sourced regularly to ensure currency.
- That written reports are reviewed thoroughly for accuracy, completeness and relevance prior to being remitted to stakeholders.

**Policy name** Privacy
**Author** Emma Spiers, National Manager, UK
**Approved by** Natalie Keating, Chief Executive Officer, UK

- That file notes within client files are maintained comprehensively and in a timely manner to ensure quality of information and currency of information.

## Quality of File Notes

File notes are a record of personal information that may have been collected, either from the individual themselves, or from an authorised third party.

File notes need to accurately reflect the personal information collected.

Where opinions are sourced from third parties, it should be clearly indicated that the information is an opinion rather than an objective fact within the file note. This may be important should an individual request correction of personal information or access to personal information and may reduce future contention.

File notes should be created in a timely manner (that is, as soon as possible after the action was undertaken) to ensure that the client's file is up to date and current.

File notes should only be stored within the file held for the client to which the personal information relates.

File notes should meet The Better Health Generation' standard for file notes.

## Security of personal information

This policy section relates specifically to Australian Privacy Principle 11 – Security of personal information.

The Better Health Generation will take all reasonable steps to protect the personal information collected during the course of service delivery in order to prevent:

- Misuse, interference and loss.
- Unauthorised access, modification or disclosure.

Where this function is outsourced to an external organisation, The Better Health Generation will take sufficient steps to monitor the provider's service provision and ensure it meets the requirements of this policy.

In the circumstance that The Better Health Generation holds personal information about an individual and this information is no longer required by The Better Health Generation for any purpose for which the information may be used or disclosed, The Better Health Generation will take all reasonable steps to destroy the personal information or ensure that the personal information is de-identified.

| | |
|---|---|
| **Policy name** | Privacy |
| **Author** | Emma Spiers, National Manager, UK |
| **Approved by** | Natalie Keating, Chief Executive Officer, UK |

## Access to personal information

This policy section relates specifically to Australian Privacy Principle 12 – Access to personal information.

The Better Health Generation will, as required by the Australian Privacy Principles, provide access to personal information held by The Better Health Generation to the individual upon request, unless an exception has been deemed to exist, or unless compliance with the requirements of the Australian Privacy Principles will be at risk.

The Better Health Generation will aim to respond to requests for access to personal information within 14 days.

Access to information held by The Better Health Generation will be provided within a reasonable period after the request is made, and will be provided in a manner requested by the individual, if it is reasonable and practicable to do so.

## Acting upon legal representatives request for information

Group recognise the professional requirements and standards of solicitors and legal representatives, and therefore, will respond promptly to requests from legal representatives concerning access to their client's personal information.

The Better Health Generation will ensure that client information released to legal parties, upon request:

- Is confined to personal information of the client concerned.
- Excludes any information relating to our activities and functions, held within the client file that does not also contain personal information of the client.

The Better Health Generation will not delay response to requests for personal information by legal representatives on any grounds (including requesting a subpoena or citing an authorisation from the client), unless it is deemed that compliance with one or more of the Australian Privacy principles may be at risk.

## Restricting or refusal of access to personal information (exceptions)

The Better Health Generation recognise and will restrict access to personal information where it has been appropriately deemed that the following exceptions exist:

- The Better Health Generation reasonably believes that giving access would pose a serious threat to the life, health or safety of an individual, or to public health or public safety; or

**Policy name** Privacy
**Author** Emma Spiers, National Manager, UK
**Approved by** Natalie Keating, Chief Executive Officer, UK

- Giving access would have an unreasonable impact on the privacy of other individuals; or
- The request for access is frivolous or vexatious; or
- The personal information relates to existing or anticipated legal proceedings between The Better Health Generation and the individual, and would not be accessible by the process of discovery in those proceedings; or
- Giving access would reveal the intentions of The Better Health Generation in relation to negotiations with the individual in such a way as to prejudice those negotiations; or
- Giving access would be unlawful; or
- Denying access is required or authorised by or under Australian law or a Court/Tribunal order; or
- Both of the following apply:
- The entity has reason to suspect that unlawful activity, or misconduct of a serious nature, that relates to The Better Health Generation's functions or activities has been, is being, or may be engaged in;
- ii. Giving access would be likely to prejudice the taking of appropriate action in relation to the matter; or
- Giving access would be likely to prejudice one or more enforcement related activities conducted by, or on behalf of, an enforcement body; or
- Giving access would reveal evaluative information generated within The Better Health Generation in connection with a commercially sensitive decision-making process.

If The Better Health Generation refuses to give access to the personal information for any of the abovementioned reasons, or refuses to give access in the manner requested by the individual, The Better Health Generation will take such steps, if any, as are reasonable in the circumstances, to give access in a way that meets the needs of The Better Health Generation and the individual. Access may be given through the use of a mutually agreed intermediary.

Where access to personal information has been refused, The Better Health Generation will give the individual a written notice that sets out:

- The reason for the refusal except to the extent that, having regard to the grounds for the refusal, it would be unreasonable do so; and
- The mechanisms available to complain about the refusal; and
- Any other matter prescribed by the regulations.

**Policy name** Privacy
**Author** Emma Spiers, National Manager, UK
**Approved by** Natalie Keating, Chief Executive Officer, UK

Where The Better Health Generation refuses to provide access to personal information due to the likelihood that access may reveal evaluative information generated within The Better Health Generation in connection with a commercially sensitive decision-making process, the reasons for the refusal may include an explanation for the commercially sensitive decision.

## Cost of accessing information

The Better Health Generation will forego any reasonable costs associated with a client making a request to access to personal information for clients.

If The Better Health Generation does proceed with applying charges for giving access to personal information, the charge will not be excessive and will not involve any costs associated with the individual making the request. Additionally, the charge will not exceed the actual cost incurred by The Better Health Generation and will not include:

- Costs associated with obtaining legal or other advice.
- Costs for consulting with the client regarding how access might be given.

The Better Health Generation may choose to waive, reduce or share costs associated with giving access to personal information.

The Better Health Generation will clearly communicate any likely costs with the client before the charge is imposed.

## Correction of personal information

This policy section relates specifically to Australian Privacy Principle 13 – correction of personal information.

Where The Better Health Generation holds personal information about an individual; and is satisfied that, having regard to a purpose for which the information is held, the information is inaccurate, out of date, incomplete, irrelevant or misleading; or the individual requests The Better Health Generation to correct the information, Better Health Inc will take all reasonable steps, if any, to correct that information to ensure that the information is accurate, up to date, complete, relevant and not misleading.

## Notification of correction to third parties

**Policy name** Privacy
**Author** Emma Spiers, National Manager, UK
**Approved by** Natalie Keating, Chief Executive Officer, UK

If The Better Health Generation corrects personal information about an individual that The Better Health Generation previously disclosed to another stakeholder; and the individual requests The Better Health Generation to notify the other stakeholder of the correction, The Better Health Generation will take such steps, if any, as are reasonable in the circumstances, to give that notification, unless it is impracticable or unlawful to do so.

## Refusal to correct information

Where The Better Health Generation may refuse to correct the personal information as requested by the individual, The Better Health Generation must give the individual a written notice that sets out:

- The reasons for the refusal except to the extent that it would be unreasonable to do so; and
- The mechanisms available to complain about the refusal; and
- Any other matter prescribed by the regulations.

Request to associate a statement:

If for particular reasons The Better Health Generation refuses to correct the personal information as requested by the individual; and the individual requests The Better Health Generation to associate with the personal information a statement that the information is inaccurate, out of date, incomplete, irrelevant or misleading; The Better Health Generation will take such steps as are reasonable in the circumstances to associate the statement in such a way that will make the statement apparent to the users of the personal information.

The Better Health Generation will respond efficiently and effectively to requests to associate a statement, and will respond to requests of this nature in a reasonable period of time following the request being made.

## Charges for correcting information

The Better Health Generation will not charge individuals to correct personal information.

The Better Health Generation will not charge individuals to make a request to associate a statement.

Where correction of information is deemed to not be the most appropriate course of action.

In accordance with the Health Records Act, 2001 (Victoria), The Better Health Generation will establish processes to remove incorrect health information held for clients who are in receipt of services within the

state of Victoria, in the event that correction is determined to not be possible or not appropriate, so that the information cannot be referred to in the course of service delivery.

### Breaches of privacy by employees of The Better Health Generation

The Better Health Generation maintains adequate processes and resources in order to educate our staff surrounding their obligations under privacy legislation, and ensure all obligations under the legislation are met.

A minor breach in this policy will result in disciplinary action, at the discretion of the Executive Manager of the business unit where the breach occurred.

A severe breach of sensitive information into the public domain, particularly where the breach is a notifiable data breach, will result in a first and final warning, and termination of contract for the employee found responsible through a fair and transparent investigation process. An employee's contract may be suspended during the period of investigation.

### Employee responsibilities for reporting and recording breaches of privacy

Staff are required, under this policy, to report all breaches of privacy. In doing so, staff should utilise complaint mechanisms to formally report and record breaches. Informal reporting should also occur through the organisations management hierarchy, and should not be delayed in preference for formal reporting.

### Acting upon breaches of privacy

All breaches of privacy will be acted upon in accordance with The Better Health Generation's stakeholder feedback processes, and in accordance with this policy and its associated legislation.

### Notifiable Data Breaches Scheme

The Better Health Generation will maintain adequate processes and resources to ensure full compliance with the Notifiable Data Breaches scheme. This includes, but is not limited to:

- Adopting, and monitoring the effectiveness of, cyclical processes to ensure IT security.

**Policy name** Privacy
**Author** Emma Spiers, National Manager, UK
**Approved by** Natalie Keating, Chief Executive Officer, UK

- Timely remediation of data breaches wherever possible to mitigate potential for serious harm.
- Maintaining consistent and effective processes to assess suspected data breaches.
- Assessing suspected data breaches to identify if there is likely or actual serious harm incurred.
- Notifying individuals whose personal information is involved in a data breach, that is likely to result in serious harm, where required by legislation and deemed necessary during the assessment of the breach.

### Destruction of Personal Information

The Better Health Generation will take reasonable steps to destroy personal information that is no longer needed for its primary purpose. These steps may include:

### Paper record destruction

The Better Health Generation will adopt consistent and cyclical processes to ensure that personal information held in hard copy format is destroyed once the information is no longer required for its original intended purpose, or primary purpose.

- Client records held in hard copy format will be retained as follows:
- For 7 years from the date of last service, where the client was an adult at the time of referral, except for where the records are subject to relevant Freedom of Information legislation
- Until the client reaches the age of 25 where the client was referred to The Better Health Generation prior to them attaining the age of 18.

### Record destruction process will ensure that:

- Where the hard copy information is needed to be retained for a purpose other than the primary purpose for which it was collected, all personal information will be de-identified.
- All personal information that is identified as no longer being required for its original intended purpose will be destroyed and no copies or back up information will be retained, except for where the records are subject to relevant Freedom of Information legislation
- All outsourced organisations who are contracted to provide destruction of personal information can assure the ongoing protection of personal information and health information during the process of destruction.

| | |
|---|---|
| **Policy name** | Privacy |
| **Author** | Emma Spiers, National Manager, UK |
| **Approved by** | Natalie Keating, Chief Executive Officer, UK |

### Electronic Record Destruction

The Better Health Generation will adopt consistent and cyclical processes to ensure that electronic information which includes personal information is destroyed once the information is no longer required for its original intended purpose, or primary purpose.

Client records held in electronic copy will be retained as per the retention periods documented above for hard copy format information.

- Electronic record destruction processes will ensure the following where permitted under state based or other relevant legislation:
- All data which is considered to be personal information or health related information is irretrievably destroyed.
- All electronically held documents which contain personal or health related information are irretrievably destroyed.
- All financial information held within client files may be retained but will be de-identified.
- All performance data relating to client files may be retained but will be de-identified.

## 4. Associated Policies and Procedures

Policy: Records Management

Procedure: How to report an incident

Procedure: Data Breach Response

Procedure: Responding to a request for The Better Health Generation records

## 5. Breach of Policy

As is the case with all of The Better Health Generation policies, failure to comply with this Policy may result in disciplinary action, leading up to and including, termination of employment.

## 6. Disclaimer

This policy sets out The Better Health Generation general approach to the matters it covers but is not intended to bind The Better Health Generation. Accordingly, this policy acknowledges that The Better Health Generation may, at its absolute discretion, amend, vary or terminate the policy at any time and in any individual case, may depart from the policy wholly or in part.

**Policy name** Privacy
**Author** Emma Spiers, National Manager, UK
**Approved by** Natalie Keating, Chief Executive Officer, UK

## 1. Policy Objectives

1.1. The General Data Protection Regulation (GDPR) replaces the Data Protection Directive 95/46/EC; the Data Protection Act 1998 (the "Act"). GDPR has been designed to harmonize data privacy laws, to protect and empower all citizens data privacy and to reshape the way organizations across the region approach data privacy.

1.2. This framework balances the legitimate needs of organisations to collect and use personal data for business and other purposes against the right of individuals to respect for the privacy of their personal details.

1.3. This policy document sets out the obligations and procedures of Health 2 Employment (H2E) Ltd ("the Company") with regard to dealing with data protection and the rights of people with whom it works in respect of their personal data under GDPR

1.4. The procedures set out herein must be followed by the Company, its employees, contractors, agents, consultants, partners or other parties working on behalf of the Company.

1.5. The Company views the correct and lawful handling of personal data as key to its success and dealings with third parties. The Company shall ensure that it handles all personal data correctly and lawfully. The Company is committed not only to the letter of the law but also to the spirit of the law and places a high premium on the correct, lawful and fair handling of all personal data, respecting the legal rights, privacy and trust of all individuals with whom it deals.

1.6. The Company is registered with the Information Commissioner as a data controller under the register held by the Information Commissioner pursuant to Section 19 of GDPR.

**6.1**

**6.2**

## 2. Scope of Policy and Responsibilities

2.1. This policy applies to all employees and officers of the Company and forms part of the employment contract with employees. Its contents are to be regarded by any person as implied, collateral or express terms to any employment contract made with the Company.

2.2. It is the responsibility of all employees to ensure they are familiar with the contents of this Policy and follow the procedures and guidelines laid out herein. Non-adherence of this policy could result in disciplinary action leading up to and including termination of employment.

2.3. This policy also applies to all customers, learners and other stakeholders (internal and external) of the Company, including any person to whom the Company provides a service.

2.4. The Company takes responsibility for achieving the objectives of this Policy, and endeavours to ensure compliance with relevant legislation. The Company reserves the right to amend and update this Policy at any time.

| | |
|---|---|
| **Policy name** | Privacy |
| **Author** | Emma Spiers, National Manager, UK |
| **Approved by** | Natalie Keating, Chief Executive Officer, UK |

**6.3**

**6.4**

## 3. Key Definitions

3.1. It is necessary to consider the meaning of a relevant defined term to determine whether and how GDPR applies. The key definitions in GDPR, the meaning of these definitions and how they often relate to each other, are as follows:

3.1.1. "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;

3.1.2. is recorded as part of a relevant filing system or with the intention that it should form part of a relevant filing system;

(a) does not fall within paragraph (a), (b) or (c) but forms part of an accessible record as defined by section 68; or

(b) is recorded information held by a public authority and does not fall within any of paragraphs (a) to (d).

3.1.3. "Relevant filing system" (referred to in paragraph (c) above) is defined in GDPR as:

(a) The GDPR applies to both automated personal data and to manual filing systems where personal data are accessible according to specific criteria. This could include chronologically ordered sets of manual records containing personal data.

3.2. 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.

3.2.1. "Personal data" means data which relates to a living individual that can be identified directly or indirectly -:

(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.

Identifiers may include:

(a) name, identification number, location data or online identifier

(b) personal data that has been pseudonymised – eg key-coded – can fall within the scope of the GDPR depending on how difficult it is to attribute the pseudonym to a particular individual.

3.2.2. "Sensitive personal data" means "special categories of personal data" outlined in Article 9 of the GDPR. The personal data consists 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) genetics;

(f) biometrics (where used for ID purposes);

(g) his physical or mental health or condition;

(h) his sexual life;

(i) Sexual orientation;

(j) the committing or alleged committing by him of any offence, or any proceedings for any offence committed or alleged to have been committed by him, the disposal of such proceedings.

3.2.3. "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.

3.2.4. "Data subject" means an individual who is the subject of personal data.

3.2.5. "Data controller" means 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.

3.2.6. "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.

3.2.7. "Recipient" in relation to personal data, means a natural or legal person, public authority, agency or another body, to which the personal data are disclosed, whether a third party or not.

3.2.8. "Third party" in relation to personal data, means a natural or legal person, public authority, agency or body other than the data subject, controller, processor and persons who, under the direct authority of the controller or processor, are authorised to process personal data any person other than –

3.2.9. "Genetic data" means personal data relating to the inherited or acquired genetic characteristics of a natural person which give unique information about the physiology or the health of that natural person and which result, in particular, from an analysis of a biological sample from the natural person in question;

3.2.10. "Biometric data" means personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data;

**6.5**

**6.6**

## 2. Organisational Measures

2.1. The Company shall ensure that the following measures are taken with respect to the collection, holding and processing of personal data:

2.1.1. A designated officer ("the Designated Officer") within the Company shall be appointed with the specific responsibility of overseeing data protection and ensuring compliance with GDPR.

2.1.2. All employees, contractors, agents, consultants, partners or other parties working on behalf of the Company are made fully aware of both their individual responsibilities and the Company's responsibilities under GDPR and shall be furnished with a copy of this Policy.

2.1.3. All employees, contractors, agents, consultants, partners or other parties working on behalf of the Company handling personal data will be appropriately trained to do so.

2.1.4. All employees, contractors, agents, consultants, partners or other parties working on behalf of the Company handling personal data will be appropriately supervised.

2.1.5. Methods of collecting, holding and processing personal data shall be regularly evaluated and reviewed.

2.1.6. The Performance of those employees, contractors, agents, consultants, partners or other parties working on behalf of the Company handling personal data shall be regularly evaluated and reviewed.

2.1.7. All employees, contractors, agents, consultants, partners or other parties working on behalf of the Company handling personal data will be bound to do so in accordance

with the principles of GDPR outlined in Section 5 of this Policy. Failure by any employee to comply with the principles or this Policy shall constitute a disciplinary offence. Failure by any contractor, agent, consultant, partner or other party to comply with the principles or this Policy shall constitute a breach of contract. Failure to comply with the principles or this Policy may also constitute a criminal offence under GDPR.

2.1.8. All contractors, agents, consultants, partners or other parties working on behalf of the Company handling personal data must ensure that any and all of their employees who are involved in the processing of personal data are held to the same conditions as those relevant employees of the Company arising out of this Policy and GDPR.

2.1.9. Where any contractor, agent, consultant, partner or other party working on behalf of the Company handles personal data on our behalf we shall look for them to indemnify and hold harmless the Company against any costs, liability, damages, loss, claims or proceedings which may arise out of their failings.

**6.7**

**6.8**

## 3. Data Protection Principles

3.1. The legislation it is underpinned by a set of straightforward, common-sense principles that will ensure compliance with the law. Schedule 1 to the Data Protection Act lists the data protection principles in the following terms:

3.1.1. Personal data shall be processed fairly, lawfully and in a transparent manner.

3.1.2. Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes.

3.1.3. Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.

3.1.4. Personal data shall be accurate and, where necessary, kept up to date.

3.1.5. Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.

3.1.6. Personal data shall be processed in accordance with the rights of data subjects under this Act.

3.1.7. Appropriate technical and organizational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data

3.1.8. 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

| | |
|---|---|
| **Policy name** | Privacy |
| **Author** | Emma Spiers, National Manager, UK |
| **Approved by** | Natalie Keating, Chief Executive Officer, UK |

**6.9**

**4. Lawful Conditions for Processing Personal Data**

4.1. The first data protection principle requires, , that one or more "conditions for processing" must be satisfied in relation to the processing of personal data. Many (but not all) of these conditions relate to the purpose or purposes for which the information is intended to be used.

4.2. The conditions for processing take account of the nature of the personal data in question. The conditions that need to be met are more exacting when the information being processed is sensitive personal data, such as information about an individual's health or criminal record.

4.3. However, the view adopted by the Company is that in determining if there is a legitimate reason for processing personal data, the best approach is to focus on whether the intended use of that data is fair. If it is, then it is very likely to identify a condition for processing that fits the purpose.

4.4. Data shall not be processed unless –

- The data subject has given his or her **clear consent** to process their personal data for a specific purpose;
- the processing is necessary for a **contract** with the individual, or because specific steps are required before entering into a contract;
- The processing is necessary for compliance with any **legal obligation** to which the data controller is subject, other than an obligation imposed by contract;
- The processing is necessary in order to protect the **vital interests** of the data subject;
- 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 processing is necessary for the purposes of **legitimate interests** pursued by the data controller or by the third party or parties to whom the data is disclosed, except where the processing is unwarranted in any particular case by reason of prejudice to the rights and freedoms or legitimate interests of the data subject.

**6.10**

**5. Lawful Conditions for Processing Sensitive Personal Data**

5.1. If the information to be processed is sensitive personal data (see Key Definitions 5.1), at least one of several other conditions must also be met before the processing can comply with the first data protection principle.

- The data subject has given explicit consent to the processing of those personal data for one or more specified purposes;

- 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;
- 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;
- 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;
- processing relates to personal data which are manifestly made public by the data subject;
- processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity;
- processing is necessary for reasons of substantial public interest, on the basis of 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;
- 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 legislation or pursuant to contract with a health professional and subject to the conditions and safeguards referred to in 6. Lawful Conditions for processing personal data;
- 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 legislation which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject, in particular professional secrecy;

5.1.1. 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 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

| | |
|---|---|
| **Policy name** | Privacy |
| **Author** | Emma Spiers, National Manager, UK |
| **Approved by** | Natalie Keating, Chief Executive Officer, UK |

**6.11**

## 6. Consent

6.1. One of the conditions for processing is that the individual has consented to their personal data being collected and used in the manner and for the purposes in question.

6.2. Article 29 of GDPR defines an individual's consent as:
"…any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her;".

6.3. Consent must be unambiguous and involve a clear affirmative action (an opt-in). It specifically bans pre-ticked opt-in boxes. It also requires distinct consent options for distinct processing operations. Consent should be separate from other terms and conditions and should not generally be a precondition of signing up to a service

6.4. GDPR stipulates that consent of the data subject means any:

- freely given,
- specific,
- informed and
- unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her

6.5. If the data subject has no real choice, feels compelled to consent or will endure negative consequences if they do not consent, then consent will not be valid.

6.6. Providing information to data subjects prior to obtaining their consent is essential in order to enable them to make informed decisions, understand what they are agreeing to, and for example exercise their right to withdraw their consent. If the controller does not provide accessible information, user control becomes illusory and consent will be an invalid basis for processing

6.7. The requirement that consent must be 'specific' aims to ensure a degree of user control and transparency for the data subject.

6.8. Consent requires a statement from the data subject or a clear affirmative act which means that it must always be given through an active motion or declaration. It must be obvious that the data subject has consented to the particular processing. A "clear affirmative act" means that the data subject must have taken a deliberate action to consent to the particular processing.41 Recital 32 sets out additional guidance on this. Consent can be collected through a written or (a recorded) oral statement, including by electronic means.

6.9. Consent must also be appropriate to the age and capacity of the individual and to the particular circumstances of the case. The processing of the personal data of a child shall be lawful where the child is at least 16 years old. Where the child is below the age of 16 years,

such processing shall be lawful only if and to the extent that consent is given or authorised by the holder of parental responsibility over the child. Regarding the age limit of valid consent the GDPR provides flexibility, but this age cannot be below 13 years

6.10. Even when consent has been given, it will not necessarily last forever. Although in most cases consent will last for as long as the processing to which it relates continues, an individual may be able to withdraw consent, depending on the nature of the consent given and the circumstances in which information is collected and used. Withdrawing consent does not affect the validity of anything already done on the understanding that consent had been given.

**6.12**

**6.13**

## 7. The Companys' Consent Procedure

7.1. All members of staff who have responsibility for a caseload of customers must ensure that every customer in their caseload has completed the appropriate form(s) of consent giving consent to collect and share personal data/information. The completed form(s) should be kept in the customer file at all times.

7.2. If any customer refuses to give consent the Centre Manager should be notified immediately. The Centre Manager should then notify the appropriate Performance Improvement Manager who will seek guidance from the designated officer

7.3. All employees should be aware of the requirements set out in the Company Information and Communication Technology (ICT) Policy relating to passwords. Under no circumstances must a password be shared with any other person. The sharing of passwords would constitute a breach of Information Security and potentially breach data protection legislation, invoking the Company disciplinary procedure

**6.14**

**6.15**

## 8. Contract

8.1. Processing personal data is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract

8.2. Personal data can be lawfully processed:

- to fulfil your contractual obligations to them; or
- because they have asked you to do something before entering into a contract (eg provide a quote).

8.3. The processing must be necessary. If it is possible to do what is required want without processing their personal data, this basis will not apply.

| | |
|---|---|
| **Policy name** | Privacy |
| **Author** | Emma Spiers, National Manager, UK |
| **Approved by** | Natalie Keating, Chief Executive Officer, UK |

**6.16**

**6.17**

### 9. Legal Obligation

9.1. Processing personal data is necessary for compliance with a legal obligation to which the controller is subject

9.2. Article 6(3) requires that the legal obligation must be laid down by UK law.

**6.18**

**6.19**

### 10. Vital Interest

10.1. The processing of personal data should also be regarded as lawful where it is necessary to protect an interest which is essential for the life of the data subject or that of another natural person such as where an individual's medical history is disclosed to a hospital's A&E department treating them after a serious road accident

10.2. Processing of personal data based on the vital interest of another natural person should in principle take place only where the processing cannot be manifestly based on another legal basis

**6.20**

**6.21**

### 11. Public Task

11.1. Processing personal data is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller

11.2. This can apply if carrying out a specific task in the public interest which is laid down by law; or exercising official authority (for example, administering justice, or for exercising statutory, governmental, or other public functions) which is laid down by law.

**6.22**

**6.23**

### 12. Legitimate Interests

12.1. Processing personal data is necessary for the purposes of the legitimate interests pursued by the controller or by a third party except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child

12.2. GDPR recognises that there are legitimate reasons for processing personal data that the other conditions for processing do not specifically deal with. The "legitimate interests" condition is intended to permit such processing, provided certain requirements are met.

12.3. This can be broken down into a three part test:

| | |
|---|---|
| **Policy name** | Privacy |
| **Author** | Emma Spiers, National Manager, UK |
| **Approved by** | Natalie Keating, Chief Executive Officer, UK |

- The **Purpose test:** are you pursuing a legitimate interest? A wide range of interests may be legitimate interests. This can be the interests of the Company or the interests of third parties, and commercial interests as well as wider social benefits for example client or employee data, marketing, fraud prevention or IT security.
- The **Necessity test:** is the processing necessary for that purpose? The processing must be a targeted and proportionate way of achieving your purpose.
- The **Balancing test**: do the individual's interests override the legitimate interest? The interests of the Company must be balanced against the individual's interests. For example, the individual would not reasonably expect the Company to use data in a way that would cause them unwarranted harm, their interests are likely to override the Company

**6.24**

**6.25**

## 13. When is Processing Necessary?

13.1. Many of the lawful bases for processing depend on the processing being "necessary". This does not mean that processing always has to be essential. However, it must be a targeted and proportionate way of achieving the purpose. The lawful basis will not apply if you can reasonably achieve the purpose by some other less intrusive means

**6.26**

**6.27**

## 14. Rights of Data Subjects

14.1. The General Data Protection Regulation affords the following rights to individuals:

**14.1.1. The right to be informed**

Individuals have the right to be informed about the collection and use of their personal data. This includes including: your purposes for processing their personal data, your retention periods for that personal data, and who it will be shared with.

**14.1.2. The right of access**

Individuals have the right to access their personal data and supplementary information. The right of access allows individuals to be aware of and verify the lawfulness of the processing.

**14.1.3. The right to rectification**

The GDPR includes a right for individuals to have inaccurate personal data rectified, or completed if it is incomplete. An individual can make a request for rectification verbally or in writing. The Company has one calendar month to respond to a request. In certain circumstances the Company may refuse a request for rectification.

**14.1.4. The right to erasure**

The GDPR introduces a right for individuals to have personal data erased. The right to erasure is also known as 'the right to be forgotten'. Individuals can make a request for erasure verbally or in writing. The Company has one month to respond to a request. The right is not absolute and only applies in certain circumstances

**14.1.5. The right to restrict processing**

Individuals have the right to request the restriction or suppression of their personal data. This is not an absolute right and only applies in certain circumstances. When processing is restricted, you are permitted to store the personal data, but not use it. An individual can make a request for restriction verbally or in writing. The Company has one calendar month to respond to a request

**14.1.6. The right to data portability**

The right to data portability allows individuals to obtain and reuse their personal data for their own purposes across different services. It allows them to move, copy or transfer personal data easily from one IT environment to another in a safe and secure way, without affecting its usability. The right only applies to information an individual has provided to a controller.

**14.1.7. The right to object**

Individuals have the right to object to

- processing based on legitimate interests or the performance of a task in the public interest/exercise of official authority (including profiling);
- direct marketing (including profiling); and
- processing for purposes of scientific/historical research and statistics.

**14.1.8. Rights in relation to automated decision making and profiling.**

GDPR has provisions on

- automated individual decision-making (making a decision solely by automated means without any human involvement); and
- profiling (automated processing of personal data to evaluate certain things about an individual). Profiling can be part of an automated decision-making process.
- The GDPR applies to all automated individual decision-making and profiling. You can only carry out this type of decision-making where the decision is:
- necessary for the entry into or performance of a contract; or
- authorised by UK law applicable to the controller; or
- based on the individual's explicit consent

| | |
|---|---|
| **Policy name** | Privacy |
| **Author** | Emma Spiers, National Manager, UK |
| **Approved by** | Natalie Keating, Chief Executive Officer, UK |

**6.28**

**6.29**

## 15. Subject Access Request

15.1. As outlined in 16.1.2, a data subject may make a subject access request (SAR) by virtue of GDPR Articles 12 and 15 and Recital 63. It is most often used by individuals who want to see a copy of the information an organisation holds about them. However, the right of access goes further than this:

- told whether any personal data is being processed;
- given a description of the personal data, the reasons it is being processed, and whether it will be given to any other organisations or people;
- given a copy of the information comprising the data; and
- given details of the source of the data (where this is available).

15.2. A fee will be charged to comply with requests for further copies of the same information. The maximum fee of £10 is based on the administrative cost of providing the information.

15.3. The Company will not comply with the requests outlined in 17.2 until the fee is received. The request will not be ignored, however the individual will be contacted promptly and informed that they need to pay.

15.4. In most cases the obligation is to respond to a subject access request promptly and in any event within one calendar month of receiving it. However, some types of personal data are exempt from the right of subject access and so cannot be obtained by making a subject access request.

15.5. For a subject access request to be valid, it can be made verbally or in writing. The following points should be noted when considering validity:

- A request can be verbal or sent hardcopy, by email or fax.
- If a disabled person finds it impossible or unreasonably difficult to make a subject access request, a reasonable adjustment can be made for them under the Equality Act 2010. This could include responding in a particular format which is accessible to the disabled person, such as Braille, large print, email or audio formats. If an individual thinks a reasonable adjustment has not been made, they may make a claim under the Equality Act 2010.
- If a request does not mention GDPR specifically or even say that it is a subject access request, it is nevertheless valid and should be treated as such if it is clear that the individual is asking for their own personal data.
- A request is valid even if the individual has not sent it directly to the person who normally deals with such requests – so it is important for all staff to recognise a subject access request and treat it appropriately.

| | |
|---|---|
| **Policy name** | Privacy |
| **Author** | Emma Spiers, National Manager, UK |
| **Approved by** | Natalie Keating, Chief Executive Officer, UK |

**6.30**

**6.31**

## 16. Subject Access Request Procedure

16.1. Any internal (employee) SAR should be made directly to the HR department who will deal with the request appropriately.

16.2. Work Programme and the Work and Heath Programme – customers may make requests for their own data but requests may also be received from third parties such as local authorities, the police, solicitors or other public bodies.

16.3. Some requests may be handled as normal business. A customer's request does not need to be handled as a SAR if they ask for copies of a CV, cover letters, action plans, Consent to Share or Information Disclosure forms, previous appointment letters or Travel Expense reimbursement forms.

16.4. Customer requests for any other information retained on file or requests from third parties (including the items listed above) must be treated as potential SARs.

16.5. Requests for blank versions of any of the documents listed above must be treated as a potential Freedom of Information request (see section below).

16.6. Any SAR – i.e.– received from a Work Programme or Work and Health Programme customer should be treated as follows:

- All requests should be immediately passed to the Centre Manager.
- The Centre Manager will determine whether the information requested falls within the items listed above or if the request has been made by a third party.
- If the information requested is included in the items listed above, the Centre Manager will provide copies to the customer.
- If the information requested is not included in the items listed above or if the request has been made by a third party, the Centre Manager will notify the customer or third party in writing, that requests should be made directly to the DWP.
- The Centre Manager will provide the customer or third party with a 'Request for Personal Information Form' and give instructions that the form should be completed and returned to the nearest Jobcentre Plus office
- The Centre Manager should ensure that the customer file and MI system are updated with the request made by the customer.

16.7. If a request is received from a Prime Contractor or the DWP regarding a SAR, the Centre Manager should inform the Performance Improvement Manager and provide the information requested no later than the next working day or within the timeframe as notified by the Prime Contractor or DWP.

16.8. The police are the only third party that the Company can directly respond to if they request a customer's personal information as part of a criminal investigation or matters of national

security. Any request or contact from the police must be referred to the Finance and Services Director who will liaise with the police and inform the Prime Contractor.

16.9. Skills Division/Non-Work Programme – Any assessor/member of staff who receives a SAR from a customer should document the request in the customers file. All written requests should be copied and also kept in the customer file

16.10. The assessor/member of staff must inform the Finance and Services Director and provide an electronic copy of any written requests.

16.11. The Finance and Services Director will liaise with the MI team to update the appropriate MI system and then liaise with the assessor/member of staff to ensure the request is properly complied with.

**6.32**

**6.33**

## 17. Freedom of Information Request

17.1. The Freedom of Information Act 2000 creates a public "right of access" to information held by public authorities. A Freedom of Information (FoI) request occurs when a person requests access to information held by public bodies, including government departments such as the DWP.

17.2. The request does not need to specifically mention GDPR itself. Therefore any request for information about our business, contracts, or performance should be treated as a potential FoI request, for example (but not limited to):

- how much we are paid to deliver contracts;
- how we spend the money we receive for delivering our services;
- how many customers we have supported into work;
- how many customer complaints we have received;
- requests for blank workbooks or other templates such as client letters;
- requests for copies of our internal policies.

17.3. The Company is not permitted to respond directly to FoI requests but is obliged to send any potential FoI requests that are received to the Prime Contractor within 1 working day. This will allow the Prime Contractor to notify the DWP within 2 working days.

17.4. The Company will assist the Prime Contractor and DWP when required in developing responses to any FoI requests.

**6.34**

**6.35**

## 18. Notification to the Information Commissioner's Office

**Policy name** Privacy
**Author** Emma Spiers, National Manager, UK
**Approved by** Natalie Keating, Chief Executive Officer, UK

18.1. As a data controller, the Company is required to notify the Information Commissioner's Office that it is processing personal data. The Company is registered in the register of data controllers.

18.2. Data controllers must renew their notification with the Information Commissioner's Office on an annual basis. Failure to notify constitutes a criminal offence.

18.3. Any changes to the register must be notified to the Information Commissioner's Office within 28 days of taking place.

18.4. The Designated Officer shall be responsible for notifying and updating the Information Commissioner's Office. The Designated Officer is Jonathan Ballin, Finance and Services Director, and contact details are as follows:

Email: jonathan.ballin@enteri2i.com