General Data Protection Policy

Author	**Sarah Lloyd**
Status	**Approved**
Date Approved	**19.10.23**
Current Version	**V3**
Next Review	**October 2025**
V1	**12.10.2018**
V2	**12.10.2021**
V3	**19.10.2023**

Policy Statement

This document is a short brief on the requirements of General Data Protection Regulations (GDPR). It also covers the procedures Age UK Bournemouth, Poole, and East Dorset (AUKBPED) has adopted to comply with legal requirements, demonstrate that these procedures have been adopted, monitor our performance, and encourage good practice. This policy should be read in conjunction with the Privacy Policy

AGEUKBPED aims to be open about the type and extent of the personal data it holds. This data will only be what is necessary to fulfil its objective of promoting the well-being of older people in Bournemouth, Poole, and East Dorset area. Our interpretation of the legislation will give priority to the interests of the data subject and addressing their needs.

GDPR applies to all our activities with or on behalf of older people and to the internal operation of the charity, including all data about our staff, volunteers, and trustees.

We are all responsible to make sure we are aware of the requirements of the GDPR and our procedures.

Other documents relevant to this subject are:

• Confidentiality policy and procedures

• Use of computers and social media networks

The following guidance is not a definitive statement on the Regulations but seeks to interpret relevant points where they affect Age UK Bournemouth, Poole and East Dorset. The Regulations cover both written and computerised information and the individual's right to see such records. It is important to note that the Regulations also cover records relating to staff and volunteers. All Age UK Bournemouth, Poole and East Dorset staff are required to always follow this Data Protection Policy.

The Chief Executive Officer has overall responsibility for data protection within Age UK Bournemouth, Poole and East Dorset, but each individual processing data is acting on the controller's behalf and therefore has a legal obligation to adhere to the

Regulations.

Scope

The topics covered in the policy include:

1) Information covered by GDPR

2) AUKBPED as a data controller

3) Holding and taking care of personal data

4) Obtaining and using personal data fairly

5) Recruitment & Personnel records

6) Disclosure to a third party

7) Requests for access to personal data

8) Record keeping – storage & disposal

9) Encouraging good practice & monitoring our compliance.

Policy

INFORMATION COVERED BY GDPR

GDPR forms part of the data protection regime in the UK, together with the Data Protection Act 2018 (DPA 2018). It applies to personal data. This is information from which a living individual can be identified, either directly or indirectly (from others information held).

Personal data does not have to be written and includes visual, photographic, and other non-text data. This covers information held on the computer, other electronic equipment, paper-based records and other records (e.g., microfiche).

AUKBPED AS A DATA CONTROLLER

Organisations or individuals holding personal data are data controllers. Many data controllers including AUKBPED must notify the Information Commissioner that we are processing personal data. The Information Commissioner maintains a public register of data controllers.

The Data Protection Commission has a list of standard purposes. In addition, AUKBPED is registered for “any other purpose that is deemed necessary and appropriate to enable the charity to fulfil its objectives and be innovative and responsive.

The Chief Executive is responsible for ensuring there is valid notification in the register of data controllers

HOLDING & TAKING CARE OF PERSONAL DATA

You are only allowed to use personal data for the purposes for which it was originally obtained. The personal information you hold must be:

• Processed lawfully, fairly and in a transparent manner in relation to individuals.

Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes. Further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be incompatible with the initial purposes.

• Must be adequate, relevant, and limited to what is necessary in relation to the purposes for which they are processed.

• Accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that is inaccurate, having regards to the purposes for which they are processed, are erased or rectified without delay.

• Kept in a format which permits identification of data subjects no longer than is necessary for the purposes for which the personal data is processed. Personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisations measures required by the GDPR in order to safeguard the rights and freedoms of individuals.

• Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisation measures.

See Record Keeping Policy appendix 1, Retaining Records for policy on time limit for retaining records.

Members of staff who, as part of their roles, are required to collect and maintain personal data must take good care of the data which they hold. There are two types of security breach that AUKBPED must protect against:

(1) unauthorised access (2) data getting damaged, lost or destroyed.

The kind of Information we hold on you

We will collect, store, and use a variety of categories of personal information about you.

Personal contact details such as name, title, addresses, telephone numbers, and personal email addresses

Date of birth

Gender

Marital status and dependents

Next of kin and emergency contact information

National Insurance number

Bank account details, payroll records and tax status information

Salary, annual leave, pension, and benefits information

Start date

Location of employment or workplace

Copy of driving license

Recruitment information (including copies of the right to work documentation, references and other information included in a CV or cover letter or as part of the application form and process)

Employment records (including job titles, work history, working hours, training records and professional memberships)

Compensation history

Performance information

Disciplinary and grievance information

Information about your use of our information and communications systems

Photographs

We may also collect, store, and use the following "special categories" of more sensitive personal information: Trade union membership. Information about your health, including any medical condition, health, and sickness records. Information about criminal convictions and offences.

Situations in which we will use your personal information There are a variety of situations in which we will use the information we collect about you, and these are detailed below. We need all the categories of information on the list above to allow us to fulfil our contract with you and to enable us to comply with legal obligations. In some cases, we may use your personal information to pursue legitimate interests of our own or those of third parties, provided your interests and fundamental rights do not override those interests. The situations in which we will process your personal information are listed below.

Deciding about your recruitment or appointment. Determining the

terms on which you work for us.

Checking you are legally entitled to work in the UK.

Paying you and, if you are an employee, deducting tax and National Insurance contributions.

Providing any company benefits to you as per your contract.

Liaising with your pension provider.

Administering the contract, we have entered with you.

Business management and planning, including accounting and auditing.

Conduct performance reviews, managing performance, and determining performance requirements.

Making decisions about salary reviews and compensation.

Assessing qualifications for a particular job or task, including decisions about promotions.

Gathering evidence for possible grievance or disciplinary hearings.

Making decisions about your continued employment or engagement.

Deciding for the termination of our working relationship Education,

training, and development requirements.

Dealing with legal disputes involving you, or other employees, workers, and contractors, including accidents at work.

Ascertaining your fitness to work. Managing sickness absence.

Complying with health and safety obligations.

To prevent fraud.

To monitor your use of our information and communication systems to ensure compliance with our IT policies.

To ensure network and information security, including preventing unauthorised access to our computer and electronic communications systems and preventing malicious software distribution.

To conduct data analytics studies to review and better understand employee retention and attrition rates.

Equal opportunities monitoring

Some of the above grounds for processing will overlap and there may be several grounds which justify our use of your personal information. Where we use your personal information to pursue the legitimate interests of the business, we will only do so provided your interests, and fundamental rights do not override those interests.

If you fail to provide personal information

If you fail to provide certain information when requested, we may not be able to fulfil the contract we have entered with you (such as paying you or providing a benefit), or we may be prevented from complying with our legal obligations (such as to ensure the health and safety of our workers).

Change of purpose

We will only use your personal information for the purposes for which we collected it, unless we reasonably consider that we need to use it for another reason and that reason is compatible with the original purpose. If we need to use your personal information for an unrelated purpose, we will notify you and we will explain the legal basis which allows us to do so. Please note that we may process your personnel information without your knowledge or consent, in compliance with the above rules, where this is required or permitted by law.

Consent

Age UK Bournemouth, Poole and East Dorset must record service users' explicit consent to storing certain information, known as 'personal data' or 'special categories of personal data', on file. For the purposes of the Regulations, personal and special categories of personal data cover information relating to:

- the racial or ethnic origin of the data subject.
- his/her political opinions.
- his/her religious beliefs or other beliefs of a similar nature.
- whether he/she is a member of a trade union.
- his/her physical or mental health or condition.
- his/her sexual life.
- the commission or alleged commission by him/her of any offence.
- online identifiers such as an IP address.
- name and contact details.
- genetic and/or biometric data which can be used to identify an individual.

Special categories of personal information collected by Age UK Bournemouth, Poole and East Dorset will, in the main, relate to service users' physical and mental health.

Data is also collected on ethnicity and held confidentially for statistical purposes.

Consent is not required to store information that is not classed as personal or special categories of personal information, if only accurate data that is necessary for a service to be provided is recorded. As a rule, Age UK Bournemouth, Poole and East Dorset will always seek consent where personal or special categories of personal information are to be held. It should also be noted that where it is not reasonable to obtain consent at the time data is first recorded and the case remains open, retrospective consent should be sought at the earliest appropriate opportunity. If personal and/or special categories of personal data need to be recorded for the purpose of service provision and the service user refuses consent, the case should be referred to the Chief Operating Officer or Chief Executive Officer for advice.

Obtaining Consent

Consent may be obtained in several ways depending on the nature of the interview, and consent must be recorded on or maintained with the case records

- face-to-face.
- written.
- telephone.
- email.

For face-to-face or written consent, pro-forma should be used. It should be specific and 'granular' so that separate consent is obtained for separate things. Each consent

statement should give the person an opportunity to make an affirmative choice to agree. Tick boxes can be used but not pre-ticked boxes or any other method of default consent. For telephone consent, verbal consent should be sought and noted on the case record. A standard consent script will be used when communicating with clients. This standard script is given below. Variations of the standard script may exist for individual services where the standard script is not appropriate.

Using and storing your data

"*Everything you tell us is treated confidentially. We will securely record your personal data, which may include health, gender and ethnicity, and we share this with our partner organisations to deliver our services. We may write to you with information about our services and activities if we think this could be of interest. We will not pass on or sell your details for marketing purposes. Is this, okay?"*

Talking to others on your behalf

"*Would you like to give permission for another person/organisation to speak to us on your behalf about your situation? We may share personal and sensitive information with this person." "Thank you for providing this information; if you change your mind, you can amend or withdraw your consent preferences at any time."*

Keeping in touch by email (where appropriate)

"*We'd like to email you occasionally with details of the work we do for older people and opportunities to support us. Is this, okay?"*

For email consent, the initial response to seek consent is below

Using and storing your data

"*Everything you tell us is treated confidentially. We will securely record your personal data, which may include health, gender and ethnicity, and we share this with our partner organisations to deliver our services. We may write to you with information about our services and activities if we think this could be of interest. We will not pass on or sell your details for marketing purposes. Is this, okay?"*

Consent obtained for one purpose cannot automatically be applied to all users, e.g. where consent has been obtained from a service user in relation to information needed for the provision of that service, separate consent would be required if, for example, direct marketing of products was to be undertaken.

Preliminary verbal consent should be sought at the point of initial contact, as personal and/or special categories of personal data will need to be recorded either in an email or on a computerised recording such as CharityLog. The verbal consent is to be recorded in the appropriate fields on the computer record or stated in the email for future reference. Individuals have a right to withdraw consent at any time.

If this affects the provision of a service(s) by Age UK Bournemouth, Poole and East Dorset, then the Service Co-ordinator should discuss with the Services Manager at the earliest opportunity.

Do we need your consent to use particularly sensitive information?

We do not need your consent if we use your personal information in accordance with our written policy to carry out our legal obligations or exercise specific rights in the field of employment law. In limited circumstances, we may approach you with your written consent to allow us to process certain particularly sensitive data. If we do so, we will provide you with full details of the information that we would like and the reason we need it, so that you can carefully consider whether you wish to consent. You should be aware that it is not the condition of your contract with us that you agree to any request for consent from us. How we use particularly sensitive personal
information “Special categories" of particularly sensitive personal information require higher levels of protection. We need to have further justification for collecting, storing, and using this type of personal information. We may process special categories of personal information in the following circumstances:

How we use particularly sensitive personal information

"Special categories" of particularly sensitive personal information require higher levels of protection. We need to have further justification for collecting, storing, and using this type of personal information. We may process special categories of personal information in the following circumstances:

In limited circumstances, with your explicit written consent.

Where we need to carry out our legal obligations and in line with our policy.

Where it is needed in public interest, in relation to our occupational pension scheme, and in line with our GDPR.

Where it is needed to assess your working capacity on health grounds, subject to appropriate confidentiality safeguards. Less commonly, we may process this type of information where it is needed in relation to legal claims or where it is needed to protect your interests (or someone else's interests) and you are not capable of giving your consent, or where you have already made the information public.

Less commonly, we may process this type of information where it is needed in relation to legal claims or where it is needed to protect your interests (or someone else's interests) and you are not capable of giving your consent, or where you have already made the information public.

Information about criminal convictions

We may only use information relating to criminal convictions where the law allows us to do so. This will usually be where such processing is necessary to carry out our obligations and provided, we do so in line with our policy. We will only collect information about criminal convictions, if it is appropriate given the nature of the role and where we are legally able to do so. Where appropriate, we will collect information about criminal convictions as part of the recruitment process or we may be notified of such information directly by you during you working for us.

Less commonly, we may use information relating to criminal convictions where it is

necessary in relation to legal claims, where it is necessary to protect your interests (or someone else's interests) and you are not capable of giving your consent, or where you have already made the information public.

Ensuring the Security of Personal Information

Unlawful disclosure of personal information

• It is an offence to disclose personal information 'knowingly and recklessly' to third parties.

• It is a condition of receiving a service that all service users for whom personal details are held should provide consent allowing Age UK Bournemouth, Poole and East Dorset to hold such information

• Service users may also consent for Age UK Bournemouth, Poole and East Dorset to share personal or special categories of personal information with other helping agencies on a need-to-know basis

• A client's individual consent to share information should always be checked before disclosing personal information to another agency.

• Where such consent does not exist, information may only be disclosed if it is in connection with criminal proceedings, or to prevent substantial risk to the individual concerned. In either case permission of the Chief Executive Officer or Safeguarding Lead should first be sought.

• Personal information should only be communicated within Age UK Bournemouth, Poole and East Dorset staff and volunteer team on a strict need-to-know basis. Care should be taken that conversations containing personal or special categories of personal information may not be overheard by people who should not have access to such information.

GDPR & Retention

We will only retain your personal information for as long as necessary to fulfil the purposes we collected it for, including for the purposes of satisfying any legal, accounting, or reporting requirements. Details of retention periods for different aspects of your personal information are set out in our GDPR Retention Policy.

To determine the appropriate retention period for personal data, we consider the amount, nature, and sensitivity of the personal data, the potential risk of harm from unauthorised use or disclosure of your personal data, the purposes for which we process your personal data and whether we can achieve those purposes through other means, and the applicable legal requirements. In some circumstances we may anonymise your personal information so that it can no longer be associated with you, in which case we may use such information without further notice to you. Once you are no longer an employee, worker or contractor of the company we will keep and securely destroy your personal information in accordance with our GDPR & Retention policy or applicable laws and regulations.

Your duty to inform us of changes

It is important that the personal information we hold about you is accurate and current. Please keep informed if your personal information changes during your working relationship with us.

Unauthorised access:

Personal information must be securely stored in a locked filing cabinet. Personal data must not be kept on the desktop unless it is being processed. Such data must be kept in a closed file folder when on the desktop. When receiving clients or visitors no personal data must be visible on the desktop or computer screen. All work areas must be cleared of personal data before leaving the office.

Staff, volunteers, and trustees should only have access to personal information when this is reasonable, relevant and necessary to undertake their role within AUKBPED

Trustees do not have the right to access client records, personnel files or other personal information unless this information is relevant to a complaint, grievance, disciplinary or other formal investigation.

Very occasionally it will be necessary to remove personal information/case files or other documents from AUKBPED premises. This may be to allow records to be referred to during a meeting or conversation or to make such records available for scrutiny by a service user. Great care must be taken to ensure the security of such papers. Files removed from the office will be placed in an envelope marked 'Private & Confidential' with AUKBPED contact details on the outside and if it is necessary to leave files in a car they must be placed in the boot and not left on display. A note giving details of the file removed will be left at the office. Papers will be returned promptly.

Password protection/ Restricted Access will be used to restrict inappropriate access to personal and sensitive information.

When disposing of confidential manual files all information must be shredded.

AUKBPED have transitioned to cloud storage, it is the responsibility of each employee to follow advice from senior personnel or IT contractors to save their work on the cloud (SharePoint) which works as a back up to protect against data loss.

It each employee's responsibility to keep their machines compliant by performing regular system updates and to follow advice given by the IT contractors.

AUKBPED has installed software to protect against computer viruses. Our outsourced contractors operate 'real time' virus checks.

Measures are taken to ensure AUKBPED premises are protected from the risks of fire and theft

OBTAINING AND USING PERSONAL DATA FAIRLY

As a data controller AUKBPED must ensure that the rights of the data subjects under the legislation are preserved. These rights are as follows:

• The right to be informed.

• The right of access.

• The right to rectification.

• The right to erasure.

• The right to restrict processing.

• The right to data portability.

• The right to object.

• Rights in relation to automated decision making and profiling.

This is done by: ➢ AUKBPED notification to the Information Commissioner ➢ All service managers who obtain, store, use or destroy information must put in place measures to inform the data subject about personal information held by AUKBPED and obtain evidence of their consent (unless consent is obvious from the context in which data is collected). For one-off telephone calls this can be done by recording a verbal notification. For more complex or on-going contact with AUKCAP, this should be confirmed in writing.

Recruitment and Personnel Records

All applicants must be informed about how their personal data will be used. It is recommended that the following information is inserted: “By signing and returning this application form you consent to AUKBPED using and keeping information about you or by third parties (such as referees) relating to your application or future employment. This information will be used solely in the recruitment process. For unsuccessful candidates the information will be destroyed within 6 months unless you have consented to extend this period”.

All personnel records for staff and volunteers must be treated as sensitive personal information. Service managers holding personal data about staff or volunteers must take particular care of the security of this information. Sickness and absence records must be held separately and securely.

Disclosure to a third party

Information can only legally be disclosed to a third party if it is fair under the terms of the General Data Protection Regulations.

All representatives of AUKBPED must obtain the consent of the data subject before disclosing personal information to a third party unless there are exceptional circumstances. You must carefully

consider the risks and benefits of all disclosures when these are done without the consent of the data subject.

If the data subject has withheld consent to disclosure, personal information must not be disclosed to a third party unless there is an exemption that will legally permit disclosure (e.g. legal requirement, emergency). The Chief Executive must be notified

of all cases where disclosure to a third party is planned to go ahead, and the data subject has refused consent.

You must not access personal data without the authority to do so and you must not knowingly or recklessly disclose it to third parties without meeting the requirements below.

You cannot use data for direct marketing of any goods or services if the data subject has told you not to

Disposal of paper, printing and photocopying over runs

Names, addresses, phone numbers and other information written on scrap paper are also considered to be confidential. If transferring papers from home to a client's home, or to the office for shredding, this should be done as soon as possible and avoid leaving documents in a car for any period.

When transporting documents, they should be carried out of sight.

Computers

Access to personal and special categories of personal information is restricted by password and restricted access control to authorised personnel only.

Computer monitors in the reception area, or other public areas, must be positioned in such a way so that passers-by cannot see what is being displayed. If this is not possible, then privacy screens should be used on the monitor to afford this level of protection. If working in a public area, e.g. reception, computers will be locked when left unattended.

Documents should only be stored on the server or cloud-based systems and not on individual computers.

Where computers or other mobile devices are taken for use off the premises the device will be password protected.

Cloud Computing

When commissioning cloud-based systems, Age UK Bournemouth, Poole and East Dorset will satisfy itself as to the compliance of data protection principles and robustness of the cloud-based providers.

Confidentiality

When working from home, or from some other off-site location, all data protection and confidentiality principles still apply. All computer data, e.g. documents and programmes related to work for Age UK Bournemouth, Poole and East Dorset must not be stored on a private external hard disk or computer. If documents need to be worked on at a non-networked computer, they should be saved to a USB drive which should be password protected.

Workstations in areas accessible to the public, e.g. reception, should operate a clear desk practice so that any paperwork, including paper diaries, containing personal

and/or special categories of personal data are not left out on the desk where passers-by could see it.

Any paperwork kept away from the office, such as a client's records kept at home by a worker, should be treated as confidential and kept secure as if it were held in the office. Documents should not be kept in an open view, such as on a desktop, but kept in a file in a drawer or filing cabinet. The optimum is a locked cabinet, but safely out of sight is a minimum requirement. Staff needing to take paperwork away from a client's home, due to being unable to make a required phone call during the visit, must ensure that it is returned to the client's home on the next visit.

If documents are being carried relating to several clients when on a series of home visits, the documents for other clients should be kept locked and out of sight in the boot of the car and not taken into the client's home. When carrying paper files or documents, they should be in a locked briefcase or in a folder or bag which can be securely closed or zipped up. The briefcase, folder or bag should contain Age UK Bournemouth, Poole and East Dorset contact details. Only personal data necessary for the job in hand should be taken on a visit. Care should be taken to ensure that the correct number of documents is taken away from a client's home and nothing is left behind.

Request for access to data we hold

Data subjects can ask to see virtually all the personal data you hold on them, including manual files. A Subject Access Request form shall be completed by the individual making the request to assist AGEUKBPED in locating all relevant information (see Appendix 1).

AUKBPED has one month to comply with a request, however this can be extended for up to 3 months

AUKBPED will not normally charge a fee to comply with a subject access request. However, there may be circumstances, for instance if a request is manifestly unfounded or excessive, when the organisation feels it is necessary to charge a "reasonable fee" for the administrative costs of complying with a request. We may also charge a reasonable fee if an individual requests further copies of their data following a request. In this case the fee will be equivalent to the administrative costs of providing further copies.

When receiving a request, it is important to assess whether it is fair to release the information when a third party is involved. Information can be edited or withheld to protect the identity of a third party. A third party can also be asked to consent to the disclosure.

Subject Access Request (Self)

Your Contact Details

The information you supply will be held in accordance with your rights under data protection laws. (Age UK Bournemouth, Poole and East Dorset referred to as Age UK BPED)

Title (tick box as appropriate)	Mrs ☐ Miss ☐ Ms ☐ Mr ☐ Other ☐ (please state):
First Name	
Last Name	
Any other names you may be known by (such as maiden name or any other previous names)	
Date of birth	
How do you want us to respond to your request?	By post ☐ email ☐ collection by hand ☐
Postal address	
Email address	
Any other email address(es) you may have used to contact Age UK BPED	
Is there any specific information you want? e.g. information about specific matters, or between certain dates	
Are there any specific people you require this information form? (This may not be possible if certain exemptions apply)	
Are you a current or former employee of Age UK BPED? Yes ☐ No ☐ If yes,	

Proof of Identity

To help us establish your identity, your application must be accompanied by copies of two official documents which between them show your name, date of birth and current address. For example: a copy of a passport, driver's licence, utility bill, council tax bill, or any other official document which shows your name and address.

Please send us copies only.

Before you return this form

Please check you have completed all sections of the form and have enclosed copies of the documents we have asked you to provide. When you have completed and checked this form, send it with copies of your proof of identification to sarah.lloyd@ageukbped.org.uk

Using your Information

The information you supply on this form will be held securely by Age UK BPED and will be used to locate the information you have requested. We will use your contact details to keep you informed of the progress of your request and to provide you with our response. We may be required to share some of the information you supply with other people and teams within Age UK BPED so that we can locate the information you have requested and make decisions on disclosure. We hold records of information requests and our responses for seven years.

RECORD KEEPING - STORAGE & DISPOSAL

Personal information can be held in a variety of documents, and it is important to adhere to the recommendations for storage and disposal of each category of document. Guidelines for each category see Record Keeping Policy.

ENCOURAGING GOOD PRACTICE AND MONITORING COMPLIANCE

To ensure that AUKBPED develops good data protection practice, implementation of data protection procedures will be maintained and monitored by the Senior management team and board of trustees

All staff and volunteers who have contact with personal data will be briefed to understand their responsibilities for data protection.

AUKBPED will ensure staff and volunteers are aware that the charity monitors e-mail, social media and telephone use (see policy on use of computers and social media networks).

All staff & board members will conduct all organisational business using work email addresses only.

Where personal information is shared with a volunteer or zero hour staff this will be done using AUKBPED encrypted email

Breaches of data protection should be reported to your manager, recorded and investigated. Serious breaches of AUKBPED guidance and procedures will be treated as a disciplinary offence.

MONITORING

This policy will be reviewed every 12 months.

COMPLAINTS TO THE ICO

You have the right to make a complaint at any time to the Information Commissioner's Office (ICO), the UK supervisory authority for data protection issues.

ICO can be contacted at:

Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF.
0303 123 1113
https://ico.org.uk/global/contact-us/contact-us-public/public-advice/

CHANGES TO THIS PRIVACY NOTICE

We reserve the right to update this privacy notice at any time, and we will provide you with new privacy notice when we make any substantial updates. We may also notify you in other ways from time to time about the processing of your personnel. information.