Global Switch

Job applicant privacy policy

1. About this privacy policy

1.1. This policy is designed to provide information on how relevant companies in the Global Switch Group process the personal data of job applicants (referred to as "you", "your") who apply to us for a job.

1.2. The Global Switch Group company that is the "controller" of the processing of your personal data (referred to as "we", "us" or "our") is the company stated in the vacancy or otherwise notified to you at the time you apply for a role with us. As a "controller", we are responsible for deciding why and how we process personal data about you. We take your privacy seriously and we are fully committed to protecting your personal data at all times. We will only process your personal data in accordance with, and adhere to the principles (as applicable) contained within applicable data protection laws.

1.3. This policy does not form part of any offer of employment and we may change this policy from time to time so please check this page occasionally to ensure that you are happy with any changes. Please also see Changes to this Policy below.

1.4. The Data Protection Manager ("DPM"), is responsible for ensuring that this privacy policy is maintained. The DPM can be contacted at DPM@globalswitch.com.

2. The kind of information we hold about you

2.1. "Personal data" is any information about a living individual from which they can be identified such as name, ID number, location data, any online identifier (such as IP address), or any factor specific to the physical, physiological, genetic, mental, economic or social identity of that person. It does not include data where any potential identifiers have been removed (anonymous data) or data held in an unstructured file.

2.2. There are "special categories" of more sensitive personal data which are more private in nature and therefore require a higher level of protection, such as genetic data, biometric data, information about sex life or sexual orientation, race or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership and health. For the purposes of this policy, personal data relating to criminal convictions will also fall within the description of 'special category/ies' personal data.

2.3. When we refer to "processing", this means anything from collecting, using, storing, transferring, disclosing, altering or destroying personal data.

3. How we use your personal data

3.1. We process your personal data for various reasons, relying on a variety of different bases for lawful processing under applicable data protection laws as set out below.

3.1.1. To comply with our legal obligations. This may include:

- checks for eligibility to work in the territory for which you are applying for work as required by immigration laws, such as passport and visa documentation;
- formal identification documentation relating to you, such as a passport or driving licence, to verify your identity (including your date of birth); and
- Disclosure and Barring Service checks or equivalent for the relevant territory ("DBS") where wehave a legal right or reason for doing so (for further information see paragraph 5 below).

3.1.2. To pursue our (or a third party's) legitimate interests as a business. This may include:

- your contact details such as your name, address, telephone number and personal email address which will be used to communicate with you in relation to the recruitment process;
- your CV, any education history, employment records, professional qualifications and certifications in order for us to consider your suitability for the job you are applying for;
- details of the job role you are applying for any interview notes made by us during or following an interview with you, in order to assess your suitability for that role;
- pay and benefit discussions with you to help determine whether a job offer may be made to you;
- voicemails, emails, correspondence, and other communications created, stored or transmitted by you on or to our computer or communications equipment in order to progress the application through the recruitment process;
- credit checking information in order to verify your suitability for the job you are applying for;
- CCTV footage of you onsite at any of our office and data centre locations for security reasons, for the protection of our property and for health and safety reasons; and
- network and information security data in order for us to take steps to protect your information against loss, theft or unauthorised access.

3.2. We will only use your personal data 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 data for an unrelated purpose, we will notify you and we will explain the legal basis which allows us to do so.

4. How we use your special categories data

4.1. We also collect, store and use your special category personal data for a range of reasons, relying on a variety of different bases for lawful processing under applicable data protection laws, as set out below.

4.1.1. To enable us to perform our legal obligations in respect of employment, social security, social protection law, or needed in the public interest. This may include:

- health information to assess and/or to comply with our obligations under the Equality Act 2010 (for example a requirement to make reasonable adjustments to your working conditions).

4.1.2. For occupational health reasons or where we are assessing your working capability, subject to appropriate confidentiality safeguards. This may include:

- information about your physical or mental health, or disability status, to assess whether any reasonable adjustments are required for you during the recruitment process and, where you are successful in your role application, carrying out any medical assessment required for your role, pension and any insurance benefits.

4.1.3. To establish, defend or exercise legal claims in an employment tribunal or any other court of law.

4.1.4. For statistical purposes in the public interest such as equal opportunities monitoring (for example the collection of information about race, ethnic origin, sex or religion). Any such information shall only be used, once collected, in an anonymised form for statistical purposes and will not be not used in relation to your application for employment with us.

5. Criminal convictions information

For certain roles, we have a legal right / reason, to undertake DBS checks. Where we do so, we only do so in accordance with our Data Protection Policy, the principles in applicable data protection laws, and the prevailing legislation in the area of criminal backgrounds checks as updated from time to time. For details on how long we retain criminal convictions information and how it is disposed of, please refer to Appendix 1.

6. Automated decision making

6.1. We do not envisage that any decisions will be taken about you using automated means, however we will notify you in writing if this position changes.

7. Data sharing

7.1. We may share your personal data and special category personal data internally. In particular, it may be shared with: HR employees involved in the recruitment process, employee relations and/or administration of your employment; line managers; consultants; advisers; and/or other appropriate persons who may be involved in the recruitment process for the job(s) you are applying for.

7.2. We may share your personal data with other companies within our group of companies. They may use your personal data as part of our regular reporting activities on performance, in the context of a business reorganisation or group restructuring exercise or for systems maintenance support and hosting of data.

7.3. We may share your personal data with third parties, agents, subcontractors and other organisations (as listed below) where we have a lawful basis for doing so. When we disclose your personal data to third parties, we only disclose to them any personal data that is necessary for them to provide their service. We have contracts in place with third parties in receipt of your personal data requiring them to keep your personal data secure and not to use it other than in accordance with our specific instructions.

Category of personal information	Recipient/relationship to us	Purpose of disclosure
All personal information collected	IT service providers	To support, maintain and host our information systems, including the software and hardware infrastructure required for it to operate/be accessible online and to keep a backup of your personal information. We also use online IT service providers to provide contract execution services
All personal information collected	Our legal and other professional advisers (including accounting and audit services)	To provide us with advice in relation to our business, including our legal, financial and other obligations and claims
Name, date of birth and contact details	Background check providers	To ensure the safety and security of the workforce

7.4. When we disclose your personal data to third parties, they may disclose or transfer it to other organisations in accordance with their data protection policies. This does not affect any of your data subject rights set out at paragraph 12 below. In particular, where you ask us to rectify, erase or restrict (the processing of) your personal data, we have an obligation to ensure that this instruction is passed on to any third parties whom we have disclosed your personal information to.

7.5. All our third-party service providers and other entities in the group are required to take appropriate security measures to protect your personal information in line with our policies. We do not allow our third-party service providers to use your personal data for their own purposes. We only permit them to process your personal data for specified purposes and in accordance with our instructions.

7.6. We may also share your personal data and special category personal data with other third parties for other reasons. For example: in the context of the possible sale or restructuring of the business; to provide information to a regulator; or to otherwise comply with the law. To comply with our legal obligations we may share your data with the following:

- HMRC for tax purposes; and
- Home Office for immigration purposes.

7.7. We may obtain personal data and/or special category personal data about you from third party sources, such as recruitment agencies, job boards, recruitment assessment centres, ccupational health professionals and background check providers. Where we receive such information from these third parties, we will only use it in accordance with this policy.

7.8. In some cases, they will be acting as a controller of your personal data and therefore we advise you to read their privacy policy and/or data protection policy.

8. Transferring information outside the uk and eea

8.1. We may transfer the personal data we collect about you to China or otherwise outside the UK and European Economic Area ("EEA"). This may happen where we are required to report to our shareholders. These countries may not have similar data protection laws to the UK or EEA and so may not protect the use of your personal information to the same standard.

8.2. If we transfer your information from the UK or EEA to a territory outside of the UK or EEA, we will take steps to ensure that appropriate protective measures are taken with the aim of ensuring that your privacy rights continue to be protected as outlined in this policy. These steps include:

- ensuring the non-UK/non-EEA countries to which transfers are made have been deemed adequately protective of your personal information for the purposes of data protection law by the relevant bodies;
- imposing contractual obligations on the recipient of your personal information using provisions formally issued by relevant bodies for this purpose. We use these provisions to ensure that your information is protected when transferred to our group companies outside UK or EEA; or
- ensuring that the recipients are subscribed to 'international frameworks', such as the EU-US Privacy Shield that aim to ensure adequate protection.

8.3. If you require further information about these protective measures, you can request it from the DPM.

9. Data storage and security

9.1. Your personal data and special category personal data is stored in a variety of locations, including: electronically on our secure servers/in hard copy form in access-restricted, locked filing cabinets/or insert other details as appropriate.

9.2. We take appropriate technical and organisational security measures and have rules and procedures in place to guard against unauthorised access, improper use, alteration, disclosure and destruction and accidental loss of your personal data.

9.3. In addition, we limit access to your personal data to those who have a business need to know and they will only process your personal data on our instructions and subject to a duty of confidentiality.

9.4. We have put in place procedures to deal with any suspected or actual data security breach and will notify you and the relevant data protection regulator of a suspected breach where we are legally required to do so.

9.5. Whenever we propose using new technologies, or where processing is construed as 'high risk', we are obliged to carry out a data protection impact assessment which allows us to make sure appropriate security measures are always in place in relation to the processing of your personal data.

10. Data retention

10.1. We keep your personal data and special category personal data for as long as is necessary to fulfil the purposes we collected it for, including for the purposes of satisfying any legal, accounting, or reporting requirements. Information about how long we retain such personal data is set out in Appendix 1.

10.2. When applying for a job with us, we compile and keep a file containing information about you which relates to your application for a job with us. Your information will be kept secure and will be used for the purposes of your job application, as explained above.

10.3. If you are offered and you accept a job with us, your personal data will be transferred to a personnel file. Any hard copy personnel file will be kept in access-restricted, locked filing cabinets. The retention period varies depending on the role(s) which you have held during your employment with us, and your personal data will be permanently and securely deleted at the end of this retention period. You will be provided with a separate Global Switch Workforce Privacy Notice which provides details of our use and handling of your personal data if you are a member of staff.

10.4. In some circumstances we may anonymise your personal data so that it can no longer be associated with you, in which case we may use and retain such information without further notice to you, as it falls outside of the definition of personal data under applicable data protection laws.

11. Your duties

11.1. We encourage you to ensure that the personal data that we hold about you for the purposes of your application or for the purposes of considering you for any similar roles is accurate and up to date by keeping us informed of any changes to your personal data. You can update your details by contacting our DPM.

12. Your rights

12.1. You may make a formal request for access to personal data and/or special category data that we hold about you at any time. This is known as a Subject Access Request. We must respond to such a request within a certain time period, being 1 month under data protection laws applicable in Europe. Please note that, under those laws, we are permitted to extend the 1 month time period for responding by an additional 2 months where in our view your request is complex or numerous in nature. We may also charge a reasonable fee based on administrative costs where in our view your request is manifestly unfounded, excessive or a request for further copies. Alternatively, we may refuse to comply with the request in such circumstances. For further details on subject access requests and the types of request listed below, please refer to our Recognising Data Subject Requests Policy and Procedure for Handling Data Subject Access Requests which can be found on Sharepoint.

12.2. Under certain circumstances, by law you also have the right to:

12.2.1. have your personal data corrected where it is inaccurate;

12.2.2. have your personal data erased where it is no longer required. Provided that we do not have any continuing lawful reason to continue processing your personal data, we will make reasonable efforts to comply with your request;

12.2.3. have your personal data be transferred to another person in an appropriate format where we process that data in reliance on your consent and the processing is carried out by automated means;

12.2.4. withdraw your consent to processing where this is our lawful basis for doing so;

12.2.5. restrict the processing of your personal data where you believe it is unlawful for us to do so, you have objected to its use and our investigation is pending, or you require us to keep it in connection with legal proceedings; and

12.2.6. to object to the processing of your personal data, where we rely on legitimate business interests as a lawful reason for the processing of your data. You also have the right to object where we are processing your personal data for direct marketing purposes. We have a duty to investigate the matter within a reasonable time and take action where it is deemed necessary. Except for the purposes for which we are sure we can continue to process your personal data, we will temporarily stop processing your personal data in line with your objection until we have investigated the matter. If we agree that your objection is justified in accordance with your rights, we will permanently stop using your data for those purposes. Otherwise, we will provide you with our justification as to why we need to continue using your data.

12.3. The way we process your personal data and the lawful basis on which we rely to process it may affect the extent to which these rights apply. If you would like to exercise any of these rights, please address them in writing to the DPM.

12.4. We may need to request specific information from you to help us to confirm your identity and ensure your right to access the information (or to exercise any of your other rights). This is an appropriate security measure to ensure that personal data is not disclosed to any person who has no right to receive it.

12.5. In the limited circumstances where you may have provided your consent to the collection, processing and transfer of your personal data for a specific purpose, you have the right to withdraw your consent for that specific processing at any time. To withdraw your consent, please contact the DPM. Once we have received notification that you have withdrawn your consent, we will no longer process your information for the purpose or purposes you originally agreed to, unless we have another legitimate basis for doing so in law. If you withdraw your consent, our use of your personal data which was collected before your withdrawal is still lawful.

You have the right to lodge a complaint with a data protection regulator, in particular in a country you work or live or where your legal rights have been infringed. However, we encourage you to contact us before making any complaint and we will seek to resolve any issues or concerns you may have. Please see the European Data Protection Board website for contact details regarding the data protection regulators in the European Union. The relevant regulator in: the United Kingdom is the UK Information Commissioner; Hong Kong is the Office of the Privacy Commissioner for Personal Data; Singapore is the Personal Data Protection Commission; and in Australia is the Australian Information Commissioner.

12.6. Although you have the right to complain to the ICO, we encourage you to contact us first with a view to letting us help in resolving any queries or questions.

13. Questions

13.1. If you have any questions about any matter relating to data protection or the personal data and/or special category personal data that that we process about you, please contact the DPM whose details can be found at paragraph Error! Reference source not found..

14. Changes to this policy

14.1. This Policy was last updated on 27 August 2020. We may update this policy from time to time by posting a copy of the updated policy on our Websites or, if we have a record of your details, we may send you an email. Unless we state otherwise, any changes to this policy will take effect seven days after the date of our email or the date on which we post the updated policy on our Websites, whichever is earlier. If you are in the application process when any changes or updates are made to this policy, we will bring any such changes to your attention as soon as is practicable.

Appendix 1

Data category	Retention Period	Reason	Disposal
Job applications and interview records of candidates	6 months – unless following an unsuccessful application you specifically consent to us holding it for longer for the purpose of contacting you in the event that any similar jobs / roles become available from time to time.	To establish, defend against or bring potential legal claims	Electronic copies of CVs and interview records will be deleted by managers and HR. Any hard copies of such documents will be destroyed by shredder / third party document destruction company.
Criminal records information (such as DBS check results) and other background check information.	6 months	To allow relevant checks to take place and any follow up queries and/or disputes to be resolved. To comply with DBS codes of practice (in respect of the UK, as issued under section 122(2) of the Police Act 1997).	