Cohort plc

Privacy Policy – Candidate Data

FINAL
30 April 2018

Authorised by: ……

AS Thomis
Chief Executive

Change History

Version	Date	Comments
1.0	21 February 2018	Initial issue in draft
1.1	30 April 2018	Final issue

1. What is the purpose of this document?

1.1. Cohort plc (“we, “our”, “us”) is committed to protecting the privacy and security of your personal information.

1.2. This privacy notice describes how we collect and use personal information about you during the recruitment process and how we use that information during recruitment and afterwards and in accordance with the General Data Protection Regulation (GDPR).

1.3. It applies to all candidates including potential employees, workers and contractors (“you”, “your”).

1.4. Cohort plc is a "data controller". This means that we are responsible for deciding how we hold and use personal information about you. We are required under data protection legislation to notify you of the information contained in this privacy notice.

1.5. This notice applies to all candidates. We may update this notice at any time.

1.6. It is important that you read this notice, together with any other privacy notice we may provide on specific occasions when we are collecting or processing personal information about you, so that you are aware of how and why we are using such information.

2. After the recruitment process

2.1. If you are successful in being appointed to a role with us, our Privacy Policy for Staff Data will apply. A copy will be provided to you with any offer letter.

2.2. If you are unsuccessful, we will retain your personal data in accordance with our retention policy. A copy of which can be obtained from the Group Head of HR.

2.3. If, having been unsuccessful, you wish us to keep your details in case further opportunities arise in the future, you will need to provide specific consent at the time and we will agree with you how long your information can be retained for this purpose.

3. Data protection principles

3.1. We will comply with data protection law. This says that the personal information we hold about you must be:

a) Used lawfully, fairly and in a transparent way.

b) Collected only for valid purposes that we have clearly explained to you and not used in any way that is incompatible with those purposes.

c) Relevant to the purposes we have told you about and limited only to those purposes.

d) Accurate and kept up to date.

e) Kept only as long as necessary for the purposes we have told you about.

f) Kept securely.

4. The kind of information we hold about you

4.1. Personal data, or personal information, means any information about an individual from which that person can be identified. It does not include data where the identity has been removed (anonymous data).

4.2. There are "special categories" of more sensitive personal data which require a higher level of protection.

4.3. We may collect, store, and use the following categories of personal information about you:

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

b) Date of birth.

c) Gender.

d) National Insurance number.

e) Recruitment information (including copies of right to work documentation, references, interview notes and opinions taken during and following interviews and other information included in a CV or cover letter or as part of the application process).

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

g) Any test results of any tests, psychometric or other, included in the recruitment process.

h) Compensation history.

i) Information necessary to complete pre-employment security checks which are a requirement for all employees of the Cohort Group which follow the HMG Cabinet Office Baseline Personnel Security Standard (BPSS).

4.4. We may also collect, store and use the following "special categories" of more sensitive personal information:

a) Information about your health, including any medical condition, health and sickness records.

b) Genetic information and biometric data.

c) Information about criminal convictions and offences.

5. How is your personal information collected?

5.1. We typically collect personal information about employees, workers and contactors through the application and recruitment process, either directly from candidates or sometimes from an employment agency or background check provider. We may sometimes collect additional information from third parties including former employers, credit reference agencies or other background check agencies.

6. How we will use information about you

6.1. We need all the categories of information in the list above primarily because they are necessary for entering into a potential contractual relationship 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:

a) Making a decision about your recruitment or appointment.

b) Determining the terms on which you work for us.

c) Checking you are legally entitled to work in the UK.

d) Assessing qualifications for a particular job or task.

e) Dealing with legal disputes involving you.

f) Ascertaining your fitness to carry out the role.

g) Complying with health and safety obligations.

h) Satisfying our Security Clearance requirements.

Some of the above grounds for processing will overlap and there may be several grounds which justify our use of your personal information.

6.2. In terms of the legitimate interests of Cohort or of third parties, these legitimate interests will be:

a) to enable us to deal with and defend any dispute or legal proceedings;

b) to enable us to satisfy our Security Clearance requirements.

6.3. We may also use your personal information in the following situations, which are likely to be rare:

a) Where we need to protect your interests (or someone else's interests). For example, if you became seriously unwell or had an accident during the recruitment process we may need to provide a hospital with personal information about you.

b) Where it is needed in the public interest or for official purposes.

6.4. If you fail to provide certain information when requested, we may not be able to offer a role to you or we may be prevented from complying with our legal obligations (such as to ensure the health and safety of our workers).

6.5. 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.

6.6. Please note that we may process your personal information without your knowledge or consent, in compliance with the above rules, where this is required or permitted by law.

7. How we use particularly sensitive personal information

7.1. "Special categories" of particularly sensitive personal information require higher levels of protection.

7.2. 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:

a) In limited circumstances, with your explicit written consent.

b) Where we need to carry out our legal obligations and in line with our data protection policy.

c) Where it is needed in the public interest, such as for equal opportunities monitoring, and in line with our data protection policy.

d) Where it is needed to assess your working capacity on health grounds, subject to appropriate confidentiality safeguards;

e) Where it is necessary for establishing, exercising or defending legal claims;

7.3. Less commonly, we may process this type of information where it is 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. For example, if you became seriously unwell or had an accident during the recruitment process we may need to provide a hospital with medical information we are aware of.

7.4. We will use your particularly sensitive personal information in the following ways:

- We will use information about your physical or mental health, or disability status, to ensure we are able to meet your health and safety in the workplace and to assess your fitness for the role or to consider / provide appropriate adjustments during the recruitment process and in the role you are being considered for.

- We will use information about your race or national or ethnic origin, religious, philosophical or moral beliefs, or your sexual life or sexual orientation, to ensure meaningful equal opportunity monitoring and reporting.

- We may obtain your biometric data as part of our recruitment process so as to comply with right to work checks.

- We may use all special categories of data to defend legal claims.

7.5. We do not need your consent if we use special categories of 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 for 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 a condition of your contract with us that you agree to any request for consent from us.

8. Information about criminal convictions

8.1. We envisage that we will collect information about criminal convictions.

8.2. All employees of the Cohort Group must be Security Cleared as a condition of their employment.

8.3. Checks regarding criminal convictions will be performed by a third party and the information provided to us. Currently the checks are performed by Staffvetting.com Limited.

8.4. This processing is necessary to ensure we are able to carry out our obligations to the Ministry of Defence and in the interests of national security. The processing will be in accordance with our data protection policy and as set out in our Security Policy Framework. A copy of both documents can be obtained from the Group Head of HR.

8.5. The checks will be carried out in accordance with the HMG Cabinet Office Baseline Personnel Security Standard (BPSS).

8.6. We will use information about criminal convictions and offences as part of the recruitment process to establish whether or not to offer you a role.

8.7. We are allowed to use your personal information in this way to carry out our obligations in respect of contracts we hold with the Ministry of Defence (MOD) and in the interests of national security.

9. Data sharing

9.1. We may share your personal information with third parties where required by law, where it is necessary as part of entering whether to enter a working relationship with you or where we have another legitimate interest in doing so.

9.2. "Third parties" includes third-party service providers (including contractors and designated agents) and other entities within our group. The following activities are carried out by third-party service providers:

a) Criminal record checks are currently performed by Staffvetting.com Limited;

b) Our Subsidiary company, SEA performs the Security Clearance checks;

c) Recruitment agencies are sometimes involved in finding potential candidates and we share some personal data with them including feedback on candidates and information regarding the terms of any job offer.

9.3. 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.

9.4. We will share your personal information with other entities in our group as part of our regular reporting activities on company performance, in the context of a business reorganisation or group restructuring exercise, for system maintenance support and hosting of data and in carrying out our Security Clearance checks.

9.5. We may also need to share your personal information with a regulator or to otherwise comply with the law.

10. Data security

10.1. We have put in place appropriate security measures to prevent your personal information from being accidentally lost, used or accessed in an unauthorised way, altered or disclosed. In addition, we limit access to your personal information to those employees, agents, contractors and other third parties who have a business need to know. They will only process your personal information on our instructions and they are subject to a duty of confidentiality. Details of these measures may be obtained from the Group Head of HR.

10.2. We have put in place procedures to deal with any suspected data security breach and will notify you and any applicable regulator of a suspected breach where we are legally required to do so.

11. Data retention

11.1. 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 available in our retention policy which is available from the Group Head of HR.

11.2. 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.

11.3. 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 retain and securely destroy your personal information in accordance with our data retention policy.

12. Rights of access, correction, erasure, and restriction

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

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

a) **Request access** to your personal information (commonly known as a "data subject access request"). This enables you to receive a copy of the personal information we hold about you and to check that we are lawfully processing it.

b) **Request correction** of the personal information that we hold about you. This enables you to have any incomplete or inaccurate information we hold about you corrected.

c) **Request erasure** of your personal information. This enables you to ask us to delete or remove personal information where there is no good reason for us continuing to process it. You also have the right to ask us to delete or remove your personal information where you have exercised your right to object to processing (see below).

d) **Object to processing** of your personal information where we are relying on a legitimate interest (or those of a third party) and there is something about your particular situation which makes you want to object to processing on this ground. You also have the right to object where we are processing your personal information for direct marketing purposes.

e) **Request the restriction of processing** of your personal information. This enables you to ask us to suspend the processing of personal information about you, for example if you want us to establish its accuracy or the reason for processing it.

f) **Request the transfer** of your personal information to another party.

12.3. If you want to review, verify, correct or request erasure of your personal information, object to the processing of your personal data, or request that we transfer a copy of your personal information to another party, please contact the Group Head of HR in writing.

12.4. You will not have to pay a fee to access your personal information (or to exercise any of the other rights). However, we may charge a reasonable fee if your request for access is clearly unfounded or excessive. Alternatively, we may refuse to comply with the request in such circumstances.

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

13. Right to withdraw consent

13.1. In the limited circumstances where you may have provided your consent to the collection, processing and transfer of your personal information 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 Data Protection Lead or Group Head of HR. 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.

14. Responsibility for compliance

14.1. The Data Protection Lead is responsible for overseeing our compliance with this privacy notice. If you have any questions about this privacy notice or how we handle your personal information, please contact the Data Protection Lead. 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. See www.ico.org.uk

15. Changes to this privacy notice

We reserve the right to update this privacy notice at any time, and we will provide you with a 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 personal information.

If you have any questions about this privacy notice, please contact the Group Head of HR.