# JIB Data Protection and Privacy Policy

## 1 Overview

1.1 The JIB takes the security and privacy of your data seriously. We need to gather and use information or 'data' about you as part of our business and to manage our relationship with you. The JIB will comply with our legal obligations under the **EU General Data Protection Regulation 2016/679** ('GDPR') and the Data Protection Act 2018 in respect of data privacy and security. We have a duty to notify you of the information contained in this policy.

1.2 This policy applies to visitors to our websites who are referred to as "You", "Your" or "Yourself" as a **'data subject'** for the purposes of this policy. This Privacy Policy will also extend to those who have made applications to be registered with the Electrotechnical Certification Scheme (ECS), formerly the UK Register of Electricians or JIB Grading system, and for whom information is stored.

1.3 This Policy document contains information about the data which the JIB holds, the processes, retention, security, your rights and obligations. Sections of relevance are highlighted where appropriate.

1.4 The JIB has measures in place to protect the security of your data. Please see these details under section 13.6 of this Policy.

1.5 The JIB will hold data in accordance with our Data Retention Policy. We will only hold data for as long as necessary for the purposes for which we collected it. Please see these details under section 14 of this Policy.

1.6 The JIB is a '**data controller**' for the purposes of your personal data and may also be a '**data processor'** in respect of information provided by employers, training providers or other third parties through the JIB online services (such as the ECS Employer Portal). This means that we determine the purpose and means of the processing of your personal data.

1.7 It is intended that this policy is fully compliant with GDPR. If any conflict arises between those laws and this policy, the JIB intends to comply with the GDPR.

## 2 Data Protection Principles

2.1 Personal data must be processed in accordance with six '**Data Protection Principles**.' It must:

- be processed fairly, lawfully and transparently;
- be collected and processed only for specified, explicit and legitimate purposes;
- be adequate, relevant and limited to what is necessary for the purposes for which it is processed;
- be accurate and kept up to date. Any inaccurate data must be deleted or rectified without delay;
- not be kept for longer than is necessary for the purposes for which it is processed; and
- be processed securely.

We are accountable for these principles and must be able to show that we are compliant.

## 3 How we define personal data

3.1 '**Personal data**' means information which relates to a living person who can be **identified** from that data (a '**data subject**') on its own, or when taken together with other information which is likely to come into our possession. It includes any expression of opinion about the person and an indication of the intentions of us or others, in respect of that person. It does not include anonymised data.

3.2 This Policy applies to all personal data whether it is stored electronically, on paper or on other materials.

3.3 This personal data might be provided to us by you, or someone else or it could be created by us.

3.4 We will collect and use the following types of personal data about you:

- your name, address, contact details (email and telephone number) and date of birth;
- your gender;
- ECS Registration number and JIB grading (if applicable);
- information such as your ECS application form, references, qualifications and membership of any professional bodies;
- your job title and employer;
- your national insurance number;
- training records;

- your photograph and identification documents as provided;
- records relating to biometric mapping against identity documents and photographs; and
- any other category of personal data which we may notify you of from time to time.

3.5 Personal information may also be collected by users to either the JIB or the ECS website such as "cookies" or IP addresses. Information on the JIB or ECS website is collected when you fill in any forms such as when sending an enquiry or when logging into your MyECS Account.

3.6 For further information please see the JIB and ECS websites for the respective Website Privacy Statements and Conditions of Use at www.jib.org.uk or www.ecscard.org.uk.

## 4 How we define special categories of personal data

4.1 '**Special categories of personal data**' are types of personal data consisting of information as to:

- your racial or ethnic origin;
- your political opinions;
- your religious or philosophical beliefs;
- your trade union membership;
- your genetic or biometric data;
- your health;
- your sex life and sexual orientation; and
- any criminal convictions and offences.

We may hold and use any of these special categories of your personal data in accordance with the law or, with reason, for the collation of aggregate industry data. Such data will be used anonymously.

4.2 Photographs, which may fall into special categories of data, will be used for the purposes of the certification scheme in order to confirm genuine identity and to display on the ECS card and within the virtual ECS card available as a smart device application.

## 5 How we define processing

5.1 **'Processing'** means any operation which is performed on personal data such as:

- collection, recording, organisation, structuring or storage;
- adaption or alteration;
- retrieval, consultation or use;
- disclosure by transmission, dissemination or otherwise making available;
- alignment or combination; and
- restriction, destruction or erasure.

This includes processing personal data which forms part of a filing system and any automated processing.

## 6 How will we process your personal data?

6.1 The JIB will process your personal data (including special categories of personal data) in accordance with our obligations for lawful basis for processing under GDPR.

6.2 We will use your personal data for:

- performing the contract of (or for) service;
- contact regarding membership or registration, marketing (where the appropriate permissions have been granted), industry updates or other information relevant to the services being provided; or
- complying with any legal obligation; or
- if it is necessary for our legitimate interests (or for the legitimate interests of someone else). However, we can only do this if your interests and rights do not override ours. You have the right to challenge our legitimate interests and request that we stop this processing. See details of your rights in section 12 below.

6.3 We can process your personal data for these purposes without your knowledge or consent. We will not use your personal data for an unrelated purpose without telling you about it and the legal basis that we intend to rely on for processing it.

6.4 If you choose not to provide us with certain personal data you should be aware that we may not be able to carry out certain parts of the contract between us e.g. in issuing the ECS card.

## 7 Examples of when we might process your personal data

7.1 We have to process your personal data in various situations before undertaking an ECS Health, Safety and Environmental Assessment, registering for MyECS, when making an ECS application and once a registration with ECS is held.

7.2 For example:

- to carry out the process of ECS registration and JIB grading;
- to carry out to process of booking an ECS Health, Safety and Environmental Awareness Assessment;
- to provide your information for verification purposes through ECS Check or similar facility of a different name (see section 8.4);
- to confirm identification documents provided are genuine and are for the relevant person applying for their ECS card;
- to confirm identification by biometric facial recognition between any identification document provided and any photograph provided for the purposes of identity document verification services, vetting, disclosure and barring service or right to work checks, to ensure any ECS Assessments administered through the JIB's systems are being correctly undertaken by the relevant data subject, to prevent fraud or misconduct;
- to carry out any form of contract between us including where relevant, its termination;
- to carry out an investigation or procedure in relation to you or someone else where misconduct is suspected or the prevention and detection of fraud or other criminal offences;
- to determine whether we need to make reasonable adjustments to the undertaking of the ECS Health, Safety and Environmental Awareness Assessment because of your disability;
- to monitor and protect the security (including network security) of the JIB, of you, our staff, customers and others;
- monitoring compliance by you, us and others with our policies and our contractual obligations;
- to comply with employment law, immigration law, health and safety law, tax law and other laws which affect us;
- running our business and planning for the future;
- to communicate with the relevant company contact regarding membership functions;
- for the purposes of providing updates on services and products, or marketing where the relevant permissions have been granted;
- to defend the JIB in respect of any investigation or litigation and to comply with any court or tribunal orders for disclosure;
- for any other reason which we may notify you of from time to time.

7.3 We will only process special categories of your personal data (see above) in certain situations in accordance with the law. For example, we can do so if we have your explicit consent such as through an ECS application or by undertaking an ECS Assessment, such as for Health, Safety and Environmental

Awareness, as this is a necessary part of the contract. If we asked for your consent to process a special category of personal data then we would explain the reasons for our request. You do not need to consent and can withdraw consent later if you choose by contacting the Data Protection Officer at dataprotectionofficer@jib.org.uk.

7.4 We do not need your consent to process special categories of your personal data when we are processing it for the following purposes, which we may do:

- where it is necessary to protect your vital interests or those of another person where you/they are physically or legally incapable of giving consent;
- to carry out an investigation or procedure in relation to you or someone else where misconduct is suspected or the prevention and detection of fraud or other criminal offences;
- where you have made the data public;
- where processing is necessary for the establishment, exercise or defence of legal claims; and
- where processing is necessary for the purposes of occupational medicine or for the assessment of your working capacity.

7.5 We may make automated decisions about you using your personal data or use profiling in relation to you, such as through identity document confirmation, biometric mapping against identification document and photographs provided for the purposes of any ECS service or as part of any smart device App, such as for access control system integration or development of such services within ECS software. Please see the relevant terms and conditions for the applicable service for more information.

## 8 Sharing your personal data

8.1 Sometimes we might share your personal data with group companies or our contractors and agents to carry out our obligations under our contract with you or for our legitimate interests.

8.2 We require those companies to keep your personal data confidential and secure and to protect it in accordance with the law and our policies. They are only permitted to process your data for the lawful purpose for which it has been shared and in accordance with our instructions.

8.3 This includes the outsourcing of printing for ECS card production. The information provided to us by you, your Employer or your Training Provider will

be sent to the printing company with whom we have a contract for this purpose. Your information is held temporarily by this printing company and only for a maximum of 12 weeks following the production of your ECS card. Any outsourced card printing company is not permitted to pass on personal information or to transfer any information outside of the EEA.

8.4 Your data may also be shared as part of ECS online services, such as remote invigilation services for ECS assessments, where personal data needs to be confirmed for the purposes of the contract provided within software providers to confirm compliance with the rules of assessment (e.g. preventing fraud and use of artificial intelligence software for monitoring during remote assessments and for the purposes of assessment moderation). This forms part of the contract with you whereby we provide a proctored, remotely available assessment service.

8.5 Identity document verification and vetting services, such as for disclosure and barring service (DBS) or right to work checks, may be necessary and this will involve the ECS systems providing some information to third party providers for these services where they are requested by you or your employer under a contract. In such circumstances, you will be contacted directly to provide the relevant identity document needed for the particular service and this may form part of the ECS application process. You may choose whether you wish to progress with such an application and in the case of information provided by your employer, your employer will need to confirm with you the relevant provisions and details to be processed in line with their own requirements in compliance with their own legal or contractual obligations.

8.6 Where you give your explicit consent, we also provide your contact information to affinity partners, which are specifically listed as part of your ECS application. If you do opt-in to receive information from these companies about their services, your information is sent directly to that company requested through the ECS system and they will contact you by telephone or email. This is an option each time you apply or renew an ECS application and whether you opt to receive this information is a personal choice. You may manage your preferences through the MyECS portal, either by desktop or within the MyECS app.

8.7 The JIB provides a third party verification service for your ECS registration. Employers, agencies, main contractors and clients need to ensure the people who are working on their projects or sites are competent to do the job they have been engaged to do and this competency assessment will include a check of your ECS status, health, safety and environmental awareness, grading and qualifications. A Legitimate Interest Assessment explaining this process and how this benefits you, us and the wider industry is contained within Section 13.

8.8 We may also need to share your personal information where we have a legitimate interest to carry out an investigation or procedure in relation to you or someone else where misconduct is suspected or the prevention and detection of fraud or other criminal offences. This information may need to be shared with training providers, insurance services providers, the industry assessment organisation responsible for the relevant end point assessment or any other company which needs to be contacted in relation to this investigation.

8.9 The JIB also works with CSCS to provide a card verification solution; CSCS Smart Check (or any other future name of this service). This system confirms an ECS card held is genuine by either scanning a QR code within the MyECS app, scanning the physical card where such technology is in place, or by manual entry of card identification number and the name of the person as it appears on their ECS card. This data will only be available to the cardholder and should be kept secure, showing the ECS card as required for site access and management. As this process relies on the individual providing their card information for verification, the individual is providing this information to the person using CSCS Smart Check, and the CSCS Smart Check app is only confirming that the ECS card details provided are genuine and correct. No further personal detail beyond that on the ECS card is provided. Card information is not stored within the CSCS Smart Check app, or through the technology company used by CSCS for the development of this application, and the QR codes generated within the MyECS App are dynamic, changing every 10 days at most, so these cannot be reused after this period of time.

8.10 We do not send your personal data outside the European Economic Area. If this changes, you will be notified of this and the protections which are in place to protect the security of your data will be explained.

8.11 Information held by the JIB is stored in the JIB network on servers located in the UK and uses cloud-based software providers with geo-replication and applicable security measures. Reference to security measures is contained in section 13.6.

## 9 How do we protect your data?

9.1 Everyone who works for, or on behalf of, the JIB has responsibility for ensuring data is collected, stored and handled appropriately, in line with this policy and the JIB's Data Security and Data Retention policies.

9.2 The JIB's Data Protection Officer is responsible for reviewing this policy. You should direct any questions in relation to this policy or data protection to the Data Protection Officer at dataprotectionofficer@jib.org.uk.

9.3 You should regularly review and update your personal data. This includes telling us if your own contact details change. You can make these necessary updates by accessing your MyECS Account, or where the contact information relates to JIB company membership, by email at membership@jib.org.uk.

9.4 Your MyECS Account also allows you to opt in or opt out of marketing services.

9.5 You should use strong passwords for this MyECS Account to prevent others from accessing your information.

9.6 Your data is held securely on the JIB's database. This database is only accessible to a limited number of JIB and ECS staff who have completed data protection training.

9.7 The JIB will ensure the proper data sharing agreements are in place prior to sharing your personal data with our partners where necessary. These agreements may be formed through the access to particular JIB owned systems under contract which set out the obligations to be met in relation to use of such a system that may disclose personal information and form contractual terms and conditions of use.

## 10 How to deal with data breaches

10.1 We have robust measures in place to minimise and prevent data breaches from taking place. Should a breach of personal data occur (whether in respect of you or someone else) then we must take notes and keep evidence of that breach. If the breach is likely to result in a risk to the rights and freedoms of individuals then we must also notify the Information Commissioner's Office within 72 hours.

10.2 If you are aware of a data breach you must contact the Data Protection Officer at dataprotectionofficer@jib.org.uk immediately and keep any evidence you have in relation to the breach.

## 11 Subject access requests

11.1 Data subjects can make a '**subject access request**' ('SAR') to find out the information we hold about them. This request must be made in writing. If you receive such a request you should forward it immediately to the Data Protection Officer who will coordinate a response.

11.2 If you would like to make a SAR in relation to your own personal data you should make this in writing to the Data Protection Officer at dataprotectionofficer@jib.org.uk. We must respond within one month unless the request is complex or numerous in which case the period in which we must respond can be extended by a further two months.

11.3 There is no fee for making a SAR. However, if your request is manifestly unfounded or excessive we may charge a reasonable administrative fee or refuse to respond to your request.

11.4 Please see the JIB Data Protection and Subject Access Request Statement available on the JIB website or by contacting the Data Protection Officer at dataprotectionofficer@jib.org.uk which sets out more information about how to make a SAR.

## 12 Your data subject rights

12.1 You have the right to information about what personal data we process, how and on what basis as set out in this policy.

12.2 You have the right to access your own personal data by way of a subject access request (see above).

12.3 You can correct any inaccuracies in your personal data. To do you should firstly log in to your MyECS Account to update the information. If this is not possible then please contact the ECS Administration Department in the first instance at administration@ecscard.org.uk. If you cannot resolve the inaccuracy via the ECS Administration Department then please email the Data Protection Officer at dataprotectionofficer@jib.org.uk.

12.4 You have the right to request that we erase your personal data where we were not entitled under the law to process it or it is no longer necessary to process it for the purpose it was collected, unless a recognised exception applies.

12.5 This would mean that if an individual wished to receive an ECS card for registration in the future following the erasure of their data, they would need to resupply originals or copies of all certificates achieved in their career. This may be a difficult task for the individual and may mean that finding appropriate work within the industry is more difficult as well.

12.6 This will be explained to any individual seeking to utilise this right to erasure, and records will need to be kept to confirm individuals have had their records erased. To do you should contact the Data Protection Officer at dataprotectionofficer@jib.org.uk.

12.7 While you are requesting that your personal data is corrected or erased or are contesting the lawfulness of our processing, you can apply for its use to be restricted while the application is made. To do so you should contact the Data Protection Officer at dataprotectionofficer@jib.org.uk.

12.8 You have the right to object to data processing where we are relying on a legitimate interest to do so and you think that your rights and interests outweigh our own and you wish us to stop. You can change your preferences through your MyECS Account.

12.9 You have the right to object if we process your personal data for the purposes of direct marketing. You can change your preferences through your MyECS Account.

12.10 You have the right to receive a copy of your personal data and to transfer your personal data to another data controller. We will not charge for this and will in most cases aim to do this within one month.

12.11 With some exceptions, you have the right not to be subjected to automated decision-making.

12.12 You have the right to be notified of a data security breach concerning your personal data.

12.13 In most situations we will not rely on your consent as a lawful ground to process your data. If we do however request your consent to the processing of your personal data for a specific purpose, you have the right not to consent or to withdraw your consent later. To withdraw your consent, you should contact the Data Protection Officer at dataprotectionofficer@jib.org.uk.

12.14 You have the right to complain to the Information Commissioner. You can do this be contacting the Information Commissioner's Office directly. Full contact details including a helpline number can be found on the Information Commissioner's Office website (www.ico.org.uk). This website has further information on your rights and our obligations.

## 13 Legitimate Interest Assessment for ECS Check and CSCS Smart Check

13.1 What is the legitimate interest?

13.1.1 The following is a legitimate interest assessment used for the purposes of sharing personal information by way of the ECS Check Service and other verification services offered by the JIB, and for CSCS Smart Check

as referenced above. Other legitimate interests may also apply and this is for the purposes of example. If you wish to know more about a particular lawful basis for processing please contact the Data Protection Officer at dataprotectionofficer@jib.org.uk.

13.1.2 The JIB has a legitimate interest in processing and sharing with third parties the personal information of individuals who are registered with ECS. Employers, agencies, main contractors and clients need to ensure the people who are working on their projects or sites are competent to do the job they have been engaged to do and this competency assessment will include a check of the data subject's name, photograph, ECS status, health, safety and environmental awareness, grading and qualifications.

13.1.3 As a matter of public safety, for auditing and reporting, and to reduce the possibility of identity fraud, it is a legitimate interest of the JIB that individuals should have their ECS card status as a checkable service to those who have signed up for the ECS Check service to ensure the proper rigour of the Scheme.

13.1.4 Similarly, those using CSCS Smart Check are able to confirm that an ECS card provided by an individual (either as a physical card checked on the information contained on the card) or through scanning the dynamic QR code within the MyECS virtual app, is genuine and is used as part of competency assessment by both employers and clients who have a legal duty to ensure the safety of all those working on their projects and within their company instruction.

13.2 Is processing necessary to achieve the Legitimate Interest?

13.2.1 The ECS Check Service requires the client, contractor or agency using this service to enter the data subject's full name as it appears on an ECS card, ECS card number and the expiry date of the ECS card, National Insurance number or a combination of the above. This is data which the data subject must have already provided to the client, contractor or agency usually by providing details of the ECS registration or through a contract compliance requirement of the data subject's employer. Information is not publicly available but is searchable. The ECS Check Service provides verification that the information provided is correct, the data subject's ECS registration is still valid (ie card expiry), photograph of the individual (if the individual has provided an auto-generation code via MyECS or if the company has signed up to the terms of use for the ECS Check Service), grading and list of qualifications held as per the ECS card image.

13.2.2 Processing this information is necessary to ensure rigour of the Scheme, check competency of workers on sites, as a matter of public safety and reduce the possibility of fraud in the industry.

13.2.3 An online service is the most effective way of verifying this personal information that is necessary as above. The online service is secure, with two factor authentication access for ECS Check. Other methods such as a telephone service would require a disproportionate effort.

13.2.4 CSCS Smart Check works by checking the details contained on the ECS card or by scanning a QR code presented as part of the individual's MyECS login through a smart device application. It is therefore paramount that individuals keep the login details for this secret. In terms of information shared, this is only the information that is contained on the ECS card and is only checkable where being provided by the individual (who is therefore consenting to such verification).

13.3 Is the Legitimate Interest balanced against the individual's rights and freedoms?

13.3.1 As a subdivision of this balancing, we consider:

- The nature of the interests
- The impact of the processing
- Any safeguards which are or could be put in place

13.4 Nature of the Interests

13.4.1 This ECS Check facility is not a publicly open register but provides searchable facilities specific to those clients, main contractors and agencies engaged in the electrical contracting industry, limited to those who sign up to the requisite service and in line with the terms and conditions of service. This requires the input of specific data for verification purposes. It would be reasonable for the data subjects to assume validity and verification checks are undertaken by their employers, main contractor or the client given the nature of ECS as a certification scheme is for verifying qualification and relate information. Therefore, this has likely been considered by the data subject when making an ECS registration application. The purpose of the Scheme is to prove to these organisations identity, validity of registration, individuals' ECS status, health, safety and environmental awareness, grading and list of qualifications held.

13.4.2 The ECS Check facility requires the data subject to provide details of their ECS registration (by way of the ECS card) to the client, contractor or agency before they can verify the relevant details through the ECS system. This may also be provided by the data subject's employer to the client or main contractor under their own legitimate interest. The ECS Check Service is for confirming and verifying the information which has already been provided by the data subject.

13.4.3 This service not only adds value and convenience for organisations in the industry, but is also of benefit to the data subject in providing this verification process for potential employers. This will expedite the recruitment process.

13.4.4 The above paragraphs should also be read for CSCS Smart Check where reference is made to the Nature of the Interests in 13.4 as the process is the same for individual supplying ECS card information to be verified.

13.5 Impact of the processing

13.5.1 Data subjects will retain the right to opt-out of the ECS Check service for employment business at any time by accessing their MyECS Account and clicking the relevant option on their account page or checking this opt-out during their initial or renewal application. However, individuals that opt-out may experience difficulty if seeking to engage in work via an employment business as they will not be searchable. Data subjects can opt-in to ECS Check by accessing their MyECS Account at any time. Data subjects cannot opt-out of the ECS Check service for clients and main contractors for the reasons as set out above in order that clients and main contractors can verify the ECS information which has been provided to them by the data subject or the data subject's employer.

13.5.2 The type of data provided through the ECS Check facility is not sensitive and does not require additional protection under GDPR. Photographs, which can in some circumstances, fall into the category of sensitive personal data, are not disclosed unless the data subject provides a generated access code either through their MyECS Account or by installing and authorising code generation through the MyECS App or where accessed through the ECS Check where the individual has provided ECS card information to be verified to the appropriate contractor, client or agency. The photograph is an essential element of ECS card information necessary for identity verification and performs one of the core functions of the ECS card.

13.5.3 The likelihood of potential harm arising from the use of these systems is minimal. Data cannot be mined from the system as organisations using ECS Check will need to input the relevant details of the data subject to verify status. As the impact is minimal and ECS card information should be verified through the online systems, there will be no option to opt-out of this service for Clients and Main Contractors as this would be counter intuitive to the purpose of a certification scheme such as ECS. Individuals may however opt-out of the service used by employment businesses. This can be done through the MyECS Portal.

13.5.4 In CSCS Smart Check, as well as the information detailed above being confirmed as genuine within the system, a photograph of the cardholder is also displayed. Again, the information is only displayed if either the card details or the scannable QR code from within the individual's MyECS smart device application is presented for verification.

13.6 Safeguards and Security

13.6.1 The following safeguards and security measures apply to all online systems provided by the JIB which involve the potential for personal information to be viewed including the MyECS Portals, both through desktop and the apps available in the App Store and Google Play Store, Employer Portal, ECS Check, Remote Invigilation, or any other future service.

13.6.2 The JIB implements appropriate technical security measures to protect data against risk presented by processing, accidental or unlawful destruction, loss, alteration, unauthorised disclosure of or access to protected data transmitted, stored or otherwise process, and have in place organisational security measures appropriate to the level of risk, including those measures as appropriate and mentioned in Articles 31(1)(a) to 32(1)(d) inclusive of the GDPR. This includes the application of security by design principles in regard to any system development.

13.6.3 The systems used by the JIB for the Employer Portal, ECS Check and undertaking health, safety and environmental assessments are undertaken through a secure version of HTTP (HTTPS) and all communications between the browser and the website are encrypted.

13.6.4 The database of information for candidates is stored behind the firewall of the JIB and is only accessible by password from those inside the system. The JIB use cloud-based services with geo-replication supporting writable primary databases and failover readable secondary databases, storied within hosting centres in Europe.

13.6.5 Using the bulk upload system for ECS applications via the online services, every application is made by HTTPS with the image included in the processes. The URL address required will only be recognised licensed organisation IP addresses. The server utilised is Transport Layer Security (TLS) 1.1.

13.6.6 Two-factor authentication is also required by users accessing the ECS Employer Portal or ECS Check to ensure only those with the relevant permissions can make these ECS applications on behalf of Data Subjects. It is the responsibility of the licensed organisation to ensure this data is accurate in line with this JIB Privacy Policy and terms and conditions for organisations licensed by the JIB to use the particular service.

13.6.7 ECS Check is the name of several online services all with secure login access requirements. A maximum number of users are permitted per organisation. Organisations are vetted before being approved and are required to sign up to terms of use which includes strict rules over the handling of this data. This access can be removed at any time if an organisation is found to be in breach of their agreement for terms of use of an ECS Check service.

13.6.8 Two factor authentication is required by using both a password for online access and a code sent via text message to the mobile telephone number held on account. For full information to be provided through the individual checking service of ECS Check, the individual must provide the employer or contractor with a generated code from within their MyECS Account or the MyECS App. A card image may be displayed covering information listed in 13.2 above where the organisation has signed up to the terms of ECS Check for organisations.

13.6.9 Considering the ECS card information required for matters of public safety, auditing and reporting, reducing fraud and increasing standards of safety within the industry through the verification of qualifications and training, it is the view of the JIB that having considered the above the JIB

has a legitimate interest in providing ECS card information through online verification systems such as ECS Check.

13.6.10 ECS services are tested at regular intervals including full website penetration testing using CREST & PTES test methodologies each year. This comprises internal and external testing. In addition, 4 vulnerability assessments are carried out each year.

## 14 Data Retention

14.1 Under the GDPR, information should only be kept where there is a legitimate purpose or reason for doing so and no more information than is necessary should be asked for and stored.

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

14.3 The JIB will regularly review:

- The nature of personal information stored;
- The length of time that information is stored for;
- The purpose in retaining the information;
- The deletion of information no longer needed for the purpose(s) for which it was stored;
- Update, archive or securely delete information if it goes out of date.

14.4 Some information is retained longer than other information. This is determined by judging:

- The current and future value of the information;
- What the information is used for and the purpose for which it was obtained;
- The costs, risks and liabilities associated with retaining the information; and
- The ease or difficulty of making sure it remains accurate and up to date.

14.5 All electronic data stored by the JIB is held securely on servers located within the UK unless listed below under 14.6.

14.6 Electrotechnical Certification Scheme (ECS) and JIB Grading

14.6.1 Employers, agencies, main contractors and clients (including public bodies) need to ensure the people working on their sites are competent to do the job for which they have been engaged and this competency assessment will include a check of the data subjects' ECS status, health, safety and environmental awareness, grading and qualifications.

14.6.2 As a matter of public safety, for auditing and reporting, and to reduce the possibility of identity fraud, it is necessary for the JIB retain these records of qualifications undertaken, as provided to the JIB by the individual concerned.

14.6.3 The JIB has several methods of retaining information for individuals' ECS records including records on the ECS Health, Safety and Environmental awareness assessment, ECS card applications and JIB grading. Information is primarily retained on a centralised database, and the information held on an individual can be viewed by logging onto the individual's MyECS Portal via the ECS website. This allows the individual to view and update relevant personal information.

14.6.4 If individuals were graded prior to 1996, the original documentation of which their grade is based (for example as an Electrician) may be stored on microfiche. This information, which will state the name, National Insurance number and provide copies of qualification certificates or other information provided by the data subject, will need to be retained to ensure rigour of the certification scheme and that correct grading has been applied as an auditable trail for grading and award of occupational discipline under ECS.

14.6.5 All information on the grading and status of individuals' certification is retained for historical, statistical and research purposes. The JIB undertakes industry wide statistical research and analysis and is regularly requested information on this basis relating to the makeup of the electrical workforce. This is in relation to age, apprenticeships, training and skill level, rates of pay, certain qualifications undertaken, retention by employers and other information relating to the composition of the workforce.

14.6.6 If an individual wishes to have their information deleted, this could be done by securely destroying the physical microfiche and deleting the ECS Card Manager record (with a record kept of the deletion of the data subject's request as permitted).

14.6.7 Retaining personal information on microfiche reduces the possibility of data being accessed online and may actually increase security, limiting

access to only those working internally for ECS or the JIB. Access can only be granted by the JIB Office Manager who retains the keys to access the records which are held in locked cabinets. Entry to this room is only monitored by entry card access.

14.6.8 The cost and time consideration of computerising these records was considered but was excessive, and would take several years to complete. This was deemed disproportionate to the potential benefits.

14.6.9 Discarding this data too soon would disadvantage the individual as they would need to resupply original certification in order to maintain their current grading or ECS registration. This would cause inconvenience but may also affect the pay rate of the individual where working under the JIB collective bargaining agreement. Likewise, the information retained is valuable for historical, statistical and research purposes.

14.6.10 The current and future value of this information is high to the JIB and wider industry in creation of necessary statistical reports, ensuring a proper audit trail for those working in the electrotechnical industry in regards to their certification and status, and to build towards an industry Licence to Practice system.

14.6.11 Individuals have the right to be forgotten as set out under sections 12.4 and 12.5. Individuals are reminded that utilising the right will mean that if the individual wishes to obtain an ECS card in the future all original documentation and certificates will need to be re-provided as these will no longer be stored and this may be to the disadvantage of the individual.

14.7 Other personal information held by the JIB

14.7.1 The JIB may also hold personal information related to company membership, the operations of the Dispute Procedure or the JIB Skills Development Fund.

14.7.2 After a period of 6 years from the date of the resolution of the Dispute or the successful application for a grant from the JIB Skills Development Fund, information relating to the individual will be anonymised or pseudonymised where the information has not been made public.

14.7.3 For example, cases which reach the Employment Tribunal or the JIB Dispute Committee are public record but many cases are resolved before this date. Records need to be retained for cases which do not reach a JIB Dispute Committee or Employment Tribunal due to the time limits on possible civil action, to ensure necessary procedure was followed,

settlement paid appropriately, for historical, statistical and research purposes on dispute resolution and industrial relations within the industry.

14.7.4 Personal information retained through applications to the JIB Skills Development Funds need to be retained to ensure instances of double claiming do not occur through the charity (as courses claimed can last up to 6 years) and for historical, statistical and research purposes on skills development and training within the industry.

14.7.5 Records are pseudonymised by reference to an individual's ECS registration number rather than shown by their name. This is not something which can provide personal information alone and can only be found by searching the JIB internal systems.

14.7.6 Personal information held for company level contacts will be retained while the company remains in membership of the JIB. Companies are encouraged to keep this information up to date on a regular basis and can contact membership@jib.org.uk to notify the Membership Department of any necessary amends.

14.7.7 Contact information is also held through the Employer Portal for ECS services, and where a company is no longer a member of the JIB, this data may be retained where it is used for a separate service such as ECS card administration and ordering. All Employer Portal companies have the ability to manage and update their own company contact preferences within the system, through the Administration function, and are encouraged to do so on a regular basis.

## 15 Staff Training for all data users

15.1 Anyone processing personal data must comply with the principles of the GDPR.

15.2 JIB and ECS members of staff, including employees, workers and self-employed under a contract of service, are appropriately trained on issues relating to data protection as part of their induction and then on regular intervals on an ongoing basis.

15.3 All data users should be made aware that:

- failure to comply with the information governance requirements contained in the JIB policies may result in disciplinary action; and

- the possibility that they may commit criminal offences if they deliberately try to access, or to disclose, personal data without authority.

15.4 Training will be provided on this policy to all data users to ensure that requests from data subjects are properly recognised. This will include guidance on how to recognise:

- a subject access request;
- a request to stop processing or objection to processing;
- any challenge to the accuracy of personal data.

15.5 The training will also:

- make employees aware of the need to check an individual's identity before providing them with personal data and the dangers of individuals attempting to obtain or alter personal data by deception; and
- inform employees how to access the JIB Privacy Policy.

15.6 More detailed training will be provided to data users who will be handling requests from data subjects to ensure that the JIB Privacy Policy is complied with. This will include reference to any relevant guidance from the ICO.

15.7 Security of personal data is of the utmost importance to the JIB.

15.8 All employees will receive training on their responsibilities under JIB's Privacy Policy and any other relevant policies relating to data breaches and incidents. This will include guidance on:

- day-to-day security (password management, access to premises, use of portable media);
- how to identify a possible data breach;
- how to report a possible data breach; and
- how staff can access the relevant policies.