



# Global Data Privacy Policy

---

## CONTENTS

	<b>Page</b>
1. INTRODUCTION – BACKGROUND AND OBJECTIVES	2
2. SCOPE AND STRUCTURE	2
3. KEY PRINCIPLES WHEN HANDLING PERSONAL DATA	3
4. SECURITY	6
5. PRIVACY BY DESIGN AND PRIVACY IMPACT ASSESSMENTS	6
6. WORKING WITH SUPPLIERS	6
7. INTERNATIONAL TRANSFERS OF DATA	7
8. RIGHTS OF INDIVIDUALS	7
9. REPORTING BREACHES	8
10. COMPLAINT HANDLING PROCEDURE	8
11. CONSEQUENCES OF FAILING TO COMPLY	8
12. AUDIT	9
13. MISCELLANEOUS	9
APPENDIX 1 - COMMON TERMS USED IN THIS POLICY	
APPENDIX 2 - PERSONAL DATA CHARTER	

## 1. INTRODUCTION – BACKGROUND AND OBJECTIVES

- 1.1 Data privacy laws exist to protect individuals' personal data, both in their private and professional capacities.
- 1.2 The Rolls-Royce group of companies (Rolls-Royce) needs to collect and use certain types of personal data about its past, prospective and/or current employees, customers, suppliers, subcontractors, visitors to our sites and websites and other individuals we engage with for a variety of business purposes. Rolls-Royce regards the lawful and correct processing of personal data held or used by us as vital to our successful operations, helping to maintain the trust of the people we deal with. Therefore, we must all treat personal data with respect, and always adhere to data privacy laws, and internal guidance.
- 1.3 This policy sets out how Rolls-Royce seeks to protect personal data and also ensures our companies, and our employees are aware of, and understand, the rules governing the use of personal data to which they have access in the course of their work.
- 1.4 For further information and support, or if you have any other comments, including any concerns that the policy is not being followed, please contact your Local Privacy Contact (LPC) or the Central Data Privacy team. Contact details can be found on our data privacy webpages: [\[link here\]](#) or email: [data.privacy@rolls-royce.com](mailto:data.privacy@rolls-royce.com).

## 2. SCOPE AND STRUCTURE

- 2.1 This policy applies to all employees and all Rolls-Royce companies. Each company member of Rolls-Royce is responsible for the personal data which it collects and processes, or that is processed on its behalf (e.g. by a third-party supplier, such as an occupational health service provider). Everyone at Rolls-Royce is responsible for ensuring compliance with this policy when handling any personal data.
- 2.2 This policy applies to all processing of personal data by Rolls-Royce companies wherever they are based, including transfers of personal data between Rolls-Royce companies. Where regional laws necessitate different or additional requirements, these will be indicated in regional appendices.
- 2.3 This policy is structured as follows:
  - 2.3.1 the main body of the policy sets out the key data privacy principles for handling personal data
  - 2.3.2 Appendix 1 contains a list of common terms used throughout this policy
  - 2.3.3 Appendix 2 sets out our Personal Data Charter, which provides more detail of our practices in relation to the collection and processing of personal data.

- 2.4 This policy supplements our other policies relating to information technology, use of Rolls-Royce devices and confidential information, which can be found on the relevant EngineRoom sites.
- 2.5 We may supplement or amend this policy with additional policies and guidelines from time to time. We will communicate any significant changes to this policy to all our companies. Latest versions of this policy are available on the Rolls-Royce data privacy webpages [[link here](#)].
- 2.6 We commit to make our Global Data Privacy policy readily available to every individual, so this policy is also published on our external webpages [[link here](#)]. Please note that some links within this document will not be accessible externally – please contact [data.privacy@rolls-royce.com](mailto:data.privacy@rolls-royce.com) if you need a copy of any such linked information.

### 3. **KEY PRINCIPLES WHEN HANDLING PERSONAL DATA**

#### 3.1 **Collection of Personal Data**

Rolls-Royce collects different types of personal data from its employees and from other individuals, for example:

- 3.1.1 in relation to employees before, during and after their employment with any Rolls-Royce company: information to support the recruitment, management and termination of employees (for example: grading, performance, sickness/absence, holiday records)
- 3.1.2 in relation to customers (where they are sole traders, individual partners in partnerships, or individuals at customer organisations): information given when placing an order, when on site, through a Rolls-Royce website, app and IT systems (which include messaging and collaboration platforms), and through attending events or participating in campaigns (for example: name, contact details, call recordings and CCTV images)
- 3.1.3 in relation to suppliers (where they are sole traders, individual partners in partnerships, or individuals at supplier organisations): in connection with the provision of goods and services, contact with such parties in the negotiation for goods and services and as part of managing such relationships, information given through a Rolls-Royce website, app and IT systems and information collected from suppliers when they attend on-site (for example: name, contact details, call recordings and CCTV images)
- 3.1.4 in relation to employees, customers, suppliers and other visitors to sites: health and safety information, sign-in information, swipe card access information and CCTV images
- 3.1.5 in relation to employees, customers, suppliers and any callers into and out of our contact/help centres: call recordings
- 3.1.6 in relation to other third parties (for example, regulators or other enforcement agencies) which Rolls-Royce companies may come into contact with during the course of its business: contact details.

### 3.2 **The seven key data privacy principles for processing any personal data**

We must always process personal data in accordance with the applicable data privacy laws and rights of individuals, and must always follow the key principles:

- 3.2.1 *Lawfulness, fairness and transparency* - only process personal data as the laws allow, and inform individuals how their data will be used. Transparency is key to data privacy. Individuals must be told how, why and on what basis their personal data is being processed, who the data may be shared with and also given an explanation of their rights in relation to their own data. This is outlined in our Fair Processing Notices and our Personal Data Charter
- 3.2.2 *Purpose limitation* - only obtain personal data for specific, explicit and legitimate purposes
- 3.2.3 *Data minimisation* - personal data must always be adequate, relevant and not excessive in relation to the purposes for which it is used
- 3.2.4 *Accuracy* - personal data must be kept accurate and up to date (and where found to be inaccurate, erased and/or rectified without delay)
- 3.2.5 *Storage limitation* - personal data must not be kept for longer than necessary for the purposes for which it is used, and only kept in a format from which individuals can be identified for as long as necessary
- 3.2.6 *Security, integrity and confidentiality* - personal data must be kept secure to prevent unauthorised processing and accidental loss, damage or destruction, using appropriate technical or organisational measures
- 3.2.7 *Accountability* - All Rolls-Royce companies are responsible for, and must be able to demonstrate, compliance with the above principles.

### 3.3 **Lawful grounds for processing personal data**

We should not process personal data unless there is a lawful ground for doing so. Employees should generally not process personal data unless:

- 3.3.1 the individual whose details are being processed has consented to this, or
- 3.3.2 the processing is necessary to perform our legal obligations or exercise legal rights, or
- 3.3.3 the processing is otherwise in our legitimate interests and does not unduly prejudice the individual's privacy<sup>1</sup>, or
- 3.3.4 another lawful basis for processing applies.

---

<sup>1</sup> If relying on this lawful basis for processing personal data, there will need to be a documented 'balance of interests' test applied to demonstrate that the privacy of individuals will not be negatively affected.

Details of the lawful grounds we rely on are set out in our various Fair Processing Notices [\[link here\]](#) and our registers of personal data processing [\[link here\]](#).

3.4 If you are in any doubt as to whether individuals should be notified as to how their personal data is processed, contact your LPC or the Central Data Privacy team.

### 3.5 **Special categories of personal data and criminal records information**

3.5.1 Special categories of personal data are afforded a higher level of protection by data privacy laws. They include data relating to racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data where this is used to identify an individual, data concerning health or data relating to a person's sex life or sexual orientation

3.5.2 Information about criminal records should also be treated as sensitive personal data, and should be handled with the same care as special categories of personal data

3.5.3 Rolls-Royce only processes special categories of personal data and criminal records information in exceptional circumstances in relation to employees, and, in relation to other parties, for health and safety and/or prevention/detection of crime purposes only. Aside from this, special categories of personal data of customers, suppliers and other third parties should not be collected or processed by Rolls-Royce without the express permission of the Central Data Privacy team.

### 3.6 **Accuracy, Adequacy, Relevance and Proportionality**

3.6.1 Personal data must be kept accurate and up to date and must be adequate, relevant and proportionate for the purpose for which it was obtained. We must never collect any personal data that we do not need

3.6.2 We must only keep personal data for as long as we need it, keeping in mind the original purpose for which it was collected. Retention policies must be followed, and personal data destroyed properly. This applies to hard copy data as well as personal data held electronically. Employees should follow our applicable retention policies and/or statutory guidelines

3.6.3 Personal data obtained for one purpose should generally not be used for other unconnected purposes, unless the individual has been informed of such purposes, and, where required, given their consent, or unless they would otherwise reasonably expect the data to be used in this way

3.6.4 Individuals may ask Rolls-Royce to correct personal data relating to them which they consider to be inaccurate. Please see section 7 below for more information on the rights of individuals.

#### 4. **SECURITY**

- 4.1 Information security is a key element of data privacy compliance and we must ensure that appropriate measures are taken to keep personal data secure, in particular from accidental or unlawful destruction, alteration, loss or unauthorised disclosure or damage. All employees must ensure they comply with this policy and all other relevant Rolls-Royce policies when using Rolls-Royce IT hardware and software, and must ensure any third parties to whom the personal data is disclosed keeps it secure.
- 4.2 Any confidential documents or documents containing personal data must not be left unattended in the work area during the day and must be securely locked away at the end of the day. Computer screens must be locked when you leave your desk. Security of documents at sites must be reviewed on a regular basis to ensure that appropriate security standards are being met.
- 4.3 Think first before forwarding extensive email chains. Check through email chains to see if there is any personal data in the chain that should not be shared more widely, and always double-check that all the email addresses of recipients are correct.

#### 5. **PRIVACY BY DESIGN AND PRIVACY IMPACT ASSESSMENTS**

- 5.1 When intending to develop a new project, product or service which involves the collection or processing of personal data, the project lead or manager must:
- (a) make sure that the provisions of this policy are taken into account from the beginning of the project
  - (b) liaise with their LPC or the Central Data Privacy team to consider whether a Privacy Impact Assessment (PIA) is required in accordance with our Privacy Impact Assessment procedure.<sup>2</sup>

#### 6. **WORKING WITH SUPPLIERS**

- 6.1 Where Rolls-Royce uses external organisations to process personal data on its behalf (e.g. for payroll processing, psychometric testing for development or recruitment purposes, share plan administration, or storage of personal data on a secure network), additional security arrangements, such as contractual terms, must be implemented with those organisations to safeguard the security of personal data. There are also mandatory legal controls which must be included in any contract with such parties.
- 6.2 Rolls-Royce's standard third party contract clauses templates [\[link here\]](#) contain appropriate data privacy clauses, which must be included in any contractual arrangement with suppliers. If a contract with a supplier involves the processing of personal data, and the standard templates are not being used, or the supplier will not accept our data privacy wording, or the type of

---

<sup>2</sup> For further information on PIAs please contact your LPC or the Central Data Privacy team (see section 1.4).

processing activity is new, employees should consult with the Central Data Privacy team to discuss other necessary steps.

- 6.3 Prior to entering into a contract with a supplier always liaise with your LPC or the Central Data Privacy team to consider whether a Privacy Impact Assessment is required.
- 6.4 Where the appointment of a supplier would also involve the transfer of personal data to a third country<sup>3</sup> or the onward sharing of personal data by the supplier with a third party who is located in a third country, further additional mandatory steps are required to be undertaken. See section 7 below. Employees should consult the Central Data Privacy team if any arrangement with a supplier will involve this transfer of personal data.

## 7. **INTERNATIONAL TRANSFERS OF DATA**

7.1 Transfers of personal data to a third country may take place if an adequacy decision exists, and/or if appropriate safeguards or an exemption applies. However, personal data transfers increase the risk of a breach of data privacy laws, so the personal data must always be adequately protected.

7.2 Adequate protection can be provided if:

7.2.1 the data protection arrangements in the destination country have been approved by the UK Government or EU Commission (as applicable). There is a list of approved countries on the ICO website (for the UK) and the EU commission website (for the EEA)

7.2.2 the recipient is a signatory to a UK or EU (as applicable) approved data privacy regime

7.2.3 the recipient is bound by a contract that ensures that the personal data concerned will be adequately protected (for example, the UK Government and the EU have approved standard forms of agreement for this purpose), and a local assessment has been undertaken which confirms that the recipient is subject to local laws which do not conflict with or prevent the same level of protection to the personal data and individuals' rights as that contained in the originating country.

7.3 Before transferring personal data, including posting it on a website or giving anyone outside of the UK/EEA access to it, if you have any doubts as to whether there is adequate protection in place, you must contact your LPC or the Central Data Privacy team. This includes any transfers or sharing between any Rolls-Royce companies.

## 8. **RIGHTS OF INDIVIDUALS**

8.1 Individuals are entitled (subject to certain exceptions) to object to the processing of their personal data, request access, rectification, deletion,

---

<sup>3</sup> 'Third Country' is a term defined in the EU GDPR; UK GDPR and Data Protection Act 2018. It essentially means that the country where the data is being sent is not situated within those geographic areas, and if the EU or UK has not deemed that country's data protection regime 'adequate', then it does not offer an essentially equivalent data protection regime to the EEA/ UK.



restriction and portability in relation to information held about them. Or, where the processing has been undertaken on the basis of consent, to withdraw their consent to that processing (at any time). All such requests should be referred immediately to the Central Data Privacy team to be actioned in line with our standard processes. This is particularly important because we must respond to a valid request within legally prescribed time limits.

- 8.2 The Personal Data Charter and our Fair Processing Notices set out further details around individual rights under data privacy laws.

## 9. **REPORTING BREACHES**

- 9.1 Employees have an obligation to report actual or potential data privacy compliance failures to the Central Data Privacy team immediately. This allows us to investigate the failure and take remedial steps if necessary. It also means that we can notify the regulatory authority/ies within the very restrictive statutory timescales where this is necessary.<sup>4</sup>
- 9.2 You may be requested to support in any such investigation, for example, by being interviewed in relation to the breach.

## 10. **COMPLAINT HANDLING PROCEDURE**

- 10.1 Individuals may complain that Rolls-Royce is not complying with this policy.
- 10.2 On receipt of a complaint, we will comply with our privacy complaint handling process. For further information regarding this, or details on how to make a complaint, please see our data privacy webpages [[link here](#)], or email: [data.privacy@rolls-royce.com](mailto:data.privacy@rolls-royce.com).

## 11. **CONSEQUENCES OF FAILING TO COMPLY**

- 11.1 Rolls-Royce takes compliance with this policy very seriously. Failure to comply puts both employees and Rolls-Royce at risk. In particular, failing to comply with this policy may lead to:
  - 11.1.1 complaints made to, or an investigation by, a supervisory authority
  - 11.1.2 significant fines for Rolls-Royce, including for breach of data privacy laws in the EEA fines of up to €20,000,000, or in the UK fines up to £17,500,000, or in each case 4% of global annual turnover, whichever is larger
  - 11.1.3 compensation claims from individuals against Rolls-Royce
  - 11.1.4 reputational damage for Rolls-Royce.
- 11.2 Negligent or deliberate breaches of this policy could result in criminal liability for employees personally. There are a number of criminal offences which can

---

<sup>4</sup> It is important that employees contact the Central Data Privacy team immediately as, in general, a notification of a data breach to the supervisory authority needs to be made without undue delay and, where feasible, not later than 72 hours after we have become aware of it, unless the breach is unlikely to result in a risk to the rights and freedoms of individuals. This all needs to be assessed and documented by the Central Data Privacy team within the set time frame.

be committed in connection with personal data. Employees may be personally liable for these offences and may face fines and even, in some cases, imprisonment.

11.3 Failure to comply with this policy may lead to disciplinary action, which may result in dismissal.

11.4 Any breaches of this policy should be reported to the Central Data Privacy team immediately.

## 12. **AUDIT**

12.1 We will audit our compliance with this policy in accordance with our internal audit programme.

## 13. **MISCELLANEOUS**

13.1 This policy is managed and maintained by the Rolls-Royce Central Data Privacy team (see section 1.4 for contact details).

13.2 Where local law requires a higher level of protection for personal data, the local law will take precedence over this policy. In any event, personal data must always be processed in compliance with local laws and we will not be responsible for a breach of this policy to the extent that compliance is prevented by local laws.

13.3 Where any Rolls-Royce company believes that local laws prevent it from complying with this policy and would have a substantial adverse effect on the protections provided by this policy, it shall promptly inform the Chief Privacy Officer (except where prohibited by a law enforcement authority, such as prohibition under criminal law to preserve the confidentiality of a law enforcement investigation).

13.4 Where there is conflict between local laws and this policy, the Chief Privacy Officer will make a responsible decision about what action to take and in event of any doubt will consult with the relevant supervising authority. The Chief Privacy Officer will notify the relevant supervising authority of such conflict, where required.

## APPENDIX 1 - COMMON TERMS USED IN THIS POLICY

**Chief Privacy Officer (CPO):** means the individual whose contact details are provided by Rolls-Royce PLC on the data privacy webpages.

**consent:** means the explicit and freely given specific and informed consent given by an appropriate method, either by a statement or by a clear positive action by the individual.<sup>5</sup>

**controller:** this is defined in data privacy law as being the entity which decides why and how personal data will be collected and processed. Usually this will be the relevant Rolls-Royce company.

**data privacy law/s:** means data protection, privacy or confidentiality law/s or regulation/s applicable in any relevant jurisdiction in which we collect and process personal data, including in the European Union and the EEA, the General Data Protection Regulation (EU) 2016/679 (GDPR), or in the United Kingdom the GDPR as it now forms UK law (UK GDPR).

**individual/s:** means a person who can be identified, directly or indirectly, in particular by reference to an identification number, or to one or more factors specific to physical, physiological, mental, economic, cultural or social identity whose personal data is processed.

**EEA:** means the European Economic Area.

**employee:** means someone who works directly for Rolls-Royce under an employment contract, either permanent or fixed term, or who is employed by Rolls-Royce on an ad-hoc basis.

**established:** in a jurisdiction means a company which is (i) a body corporate, being incorporated under the law of that jurisdiction; (ii) a partnership or other unincorporated association being formed under the law of, or any part of, that jurisdiction; or (iii) any other person who does not fall within (i) or (ii) above, but maintains in that jurisdiction an office, branch or agency through which they carry on any business activity, or a regular practice.

**local law/s:** means the law/s in the jurisdiction in which a Rolls-Royce company is established and any other law to which they are subject.

**personal data:** means any information relating to an identified or identifiable natural person/s (**individual/s**).

**policy or Global Data Privacy Policy:** means this Global Data Privacy Policy together with its appendices.

**process/processing/processed:** means any activity involving personal data, whether or not by automatic means, such as collection, recording, organisation, manipulation, storage, adaptation or alteration, retrieval, consultation, use, disclosure by

---

<sup>5</sup> Different countries have different requirements in relation to evidencing consent, so always check with your LPC or the Central Data Privacy team.

transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction.

**processor:** means a natural or legal person, public authority, agency or any other body which processes personal data on behalf of the controller.

**regulatory authority/regulator:** means any local regulator which is competent to handle data privacy issues, unless specifically defined otherwise in the text. The term is used interchangeably with supervisory authority.

**special personal data:** is defined in privacy laws and includes data that refers directly or indirectly to the racial or ethnic origin, political opinions, philosophical or religious opinions, trade union memberships, health or sexual life and orientations, and biometric information.

**supervisory authority:** means any local regulator which is competent to handle data privacy issues. The term is used interchangeably with regulatory authority/regulator.

**third country:** is a term defined in the EU GDPR; UK GDPR and Data Protection Act 2018. It essentially means that the country where the data is being sent is not situated within those geographic areas, and if the EU or UK has not deemed that country's data protection regime 'adequate', then it does not offer an essentially equivalent data protection regime to the EEA/ UK.

**third party:** means natural and legal persons which are not Rolls-Royce entities with whom a Rolls-Royce company has existing or planned business relations.

**transfer:** means the disclosure of personal data to third parties, the transmission of such data to third parties, or the process of making such data available to third parties in any form for inspection or retrieval.

## APPENDIX 2 - PERSONAL DATA CHARTER

### 1. Introduction

- 1.1 We need to handle personal data about you (whether you are an employee, customer, supplier or someone else such as a visitor to one of our sites) so that we can engage with you, provide or receive services to or from you and administer your personal data efficiently.
- 1.2 Rolls-Royce is committed to ensuring that your privacy is protected, and we comply with data privacy laws when we process personal data about you. This personal data charter contains the standards you can expect when we ask for, hold, share, or otherwise process, your personal data.
- 1.3 Please follow the principles set out in this charter if you handle personal data when working for us or handle personal data on our behalf.

### 2. The information we collect and how we use it

- 2.1 Under data privacy laws, we are required to explain what information we collect from you and how and why we use, or process, your personal data. We are also required to have a 'lawful basis' to process your personal data. This information is detailed in our Fair Processing Notices (FPNs) and our personal data processing registers [[link here](#)].
- 2.2 For some countries in which we collect or process personal data local laws may apply different requirements - we will advise you of any local requirements in the relevant FPN.
- 2.3 This personal data charter supplements any other FPN or privacy notice that may be provided to you from time to time.

### 3. Your privacy

- 3.1 When we ask you for personal data, we will:
  - (a) let you know if we share it with other organisations and if you can object to such data sharing, and
  - (b) not make your personal data available for commercial use without your permission.
- 3.2 We may share personal data within Rolls-Royce companies or with other bodies if it would be compatible with the purpose for which we collected it, and/or where we need to, or are permitted to do so by law. Where we need to share your information without your consent, we will always do so in accordance with the relevant data privacy laws.
- 3.3 In addition, we will make sure that:
  - (a) you know what personal data we are processing and why we need it
  - (b) the processing of your personal data is fair and lawful

- (c) methods, such as collection, destruction and handling of personal data are regularly reviewed
- (d) any personal data handling breaches are logged, fully investigated and reported to the appropriate regulator where necessary
- (e) there is a full-time Chief Privacy Officer, Central Data Privacy team (and, where applicable, a company/business specific Data Privacy Officer), and part-time Local Privacy Contacts who are fully supported by our Executive Leadership Team to oversee and ensure compliance with this policy
- (f) changes in data privacy laws are monitored and implemented as appropriate
- (g) anyone with a question about handling personal data knows where to go for advice and is supported in knowing what to do
- (h) queries about handling personal data are promptly, professionally and courteously dealt with.

3.4 We will ensure, so far as is possible, that the information held about you is accurate and, where necessary, kept up to date. However, it is your responsibility to ensure that any changes to your information held by Rolls-Royce are notified to the relevant data system owner or to [data.privacy@rolls-royce.com](mailto:data.privacy@rolls-royce.com) as soon as possible. In the absence of evidence to the contrary, we assume that the information provided by you is accurate. If there is any reasonable doubt as to the accuracy of the data, we will contact you to confirm the information. Should you inform us, or we otherwise become aware, of any inaccuracies in the information, the inaccuracies will be rectified promptly.

#### 4. **Information we will give you**

4.1 We commit to make our Global Data Privacy policy and regional appendices readily available to everyone whose personal data we collect and process.

4.2 Where we act as a controller, we will provide you with the following information in relation to any processing of your personal data:

- (a) identity of the member of the Rolls-Royce company which is acting as controller, and the details of the relevant data privacy officer or contact point
- (b) the purposes of the processing and the legal basis for the processing
- (c) the recipients or categories of recipients of the personal data, including where there are any overseas transfers and details of appropriate safeguards
- (d) if the personal data did not originate from you directly, from where we obtained it

- (e) the retention period for the personal data processing
- (f) confirmation of any rights in relation to the personal data, such as a right of access.

4.3 Where a Rolls-Royce company acts as a processor, it is the controller's responsibility to provide individuals with the above information. We will provide controllers with relevant information to enable them to meet their legal obligations to individuals.

## 5. **Legal grounds for processing personal data**

5.1 We will only process personal data on one of the following grounds:

- (a) individuals have given their consent to the processing (where consent is necessary)
- (b) the data processing is necessary for the purposes of our legitimate interests, or by the third party or parties to whom the personal data is disclosed, except where such interests are overridden by the interests or fundamental rights and freedoms of the individual
- (c) the data processing is necessary for the performance of a contract to which the individual is party, or in order to take steps at the request of the individual prior to entering into a contract
- (d) the data processing is necessary for compliance with a legal obligation to which we are subject
- (e) the data processing is in the vital interest of the individual (e.g. in a life or death situation)
- (f) the data processing is necessary for the performance of a task carried out in the public interest.

5.2 For special category personal data, we will only process this on one of the following grounds:

- (a) the individual has given explicit consent
- (b) the processing is necessary for the purposes of carrying out the obligations and specific rights of the controller in the field of employment law, in so far as it is authorised by national law providing for adequate safeguards
- (c) the processing is necessary to protect the vital interests of the individual or of another person where the individual is physically or legally incapable of giving his or her consent
- (d) the processing relates to special category personal data which has been made public by the individual
- (e) the processing is necessary for the establishment, exercise or defence of legal claims

- (f) the processing is required for the purposes of preventative medicine, medical diagnosis, the provision of care or treatment, or the management of healthcare services. In addition, where that special category personal data is processed by a health professional this is subject to national law or rules established by national competent bodies in relation to the obligation of professional secrecy, or by another person also subject to an equivalent obligation of secrecy.

## 6. **Data quality**

6.1 We will maintain effective procedures and systems to make sure that:

- (a) we do not collect excessive personal data (we will only ask for what we need, and not collect too much, or irrelevant information)
- (b) personal data is adequate, relevant, accurate and up to date for the intended purposes for which it is processed
- (c) we process personal data only for the purposes specified in this policy, any FPNs, data processing registers, any local policies or other information provided to you.

## 7. **Storage, retention and destruction**

7.1 We will only keep personal data for as long as is necessary for the relationship that we have with you (such as employing you or providing you with a service) and/or conducting our business. We may need to keep your personal data for longer than needed for the purposes described above in order to meet other legal requirements. We will maintain retention policies and procedures so that personal data is destroyed after an appropriate amount of time, except where another law requires us to keep the personal data for a certain length of time. When we delete personal data, we will do so in a secure and confidential way.

## 8. **Disclosure of your information**

8.1 We may on occasion transfer your personal data to third parties, including – but not limited to – suppliers or service providers (including suppliers who host or provide IT services and systems to us), insurers, medical advisors, professional advisors, Pension Schemes, providers of psychometric testing in limited circumstances, tax authorities, law enforcement agencies and data privacy supervisory authorities. In such circumstances we will ensure that adequate security measures are in place with any such entities, including appropriate contractual terms, particularly for any transfers to a third country.

8.2 On the termination of a contract where we are a processor, we will either return all the personal data transferred and the copies to the controller, or (according to the controller's instructions) destroy all the personal data and certify to the controller that we have done so. This is unless data privacy laws imposed upon us prevent us from returning or destroying all or part of the personal data transferred.



## 9. **Security**

- 9.1 We will maintain technical and organisational measures in relation to the personal data we hold to ensure it is kept secure. We will make sure that such measures are appropriate to the risks represented by the processing and nature of the personal data. Where appropriate, the arrangements will include provisions for 'need to know' access to the personal data.
- 9.2 We will make sure that confidentiality and security is respected at all times and appropriate diligence activities are carried out in relation to the security of personal data, both before and after we use it.
- 9.3 We will implement enhanced security measures for the processing of special category personal data, including additional safeguards as set out in data privacy laws.
- 9.4 The implementation of the principles set out in this section will be monitored by the Central Data Privacy team to make sure that the personal data processed by us, either as a controller or as a processor, is provided with a high and appropriate level of protection.

## 10. **Automated decisions**

- 10.1 When automated personal data processing may have a negative effect or a legal consequence for you, we will notify you about the occurrence of such automated decisions to protect your legitimate interests.
- 10.2 We will not evaluate or make a decision about you which significantly affects you based solely on automated processing of your personal data, unless that decision:
- (a) is taken in the course of entering into, or performing, a contract, provided the request lodged by the individual has been satisfied, or there are suitable measures to safeguard their legitimate interests
  - (b) is authorised by a law which lays down measures to safeguard the individual's legitimate interests.

## 11. **The training and guidance we give to our staff**

- 11.1 All of our employees are trained in the importance of protecting personal and special category personal data. The data privacy awareness course is part of the Rolls-Royce mandatory annual training suite.
- 11.2 Anyone working with large volumes of personal data receives more in-depth and/or specialised training.
- 11.3 There are various guidance notes, Frequently Asked Questions (FAQs) and further information in relation to all aspects of personal data handling available on our central data privacy webpages [\[link here\]](#) and regional privacy webpages which are reviewed and updated regularly.

## 12. **Your rights**

Subject to certain exceptions data privacy laws give rights to individuals in relation to the processing of their personal data. Your rights are set out as follows:

<b>Right</b>	<b>Description</b>
<b>To be informed</b>	A right to be informed about the personal information we hold about you.
<b>Of access</b>	A right to access the personal information we hold about you.
<b>To rectification</b>	A right to require us to rectify any factually inaccurate personal information we hold about you.
<b>To erasure</b>	A right to ask us to delete the personal information we hold about you. This right will only apply where (for example): <ul style="list-style-type: none"><li>• we no longer need to use the personal information to achieve the purpose we collected it for</li><li>• where you withdraw your consent if we are using your personal information based on your consent, or</li><li>• where you object to the way we process your data (in line with Right To Object as explained below).</li></ul>
<b>To restrict processing</b>	In certain circumstances, a right to restrict our processing of the personal information we hold about you. This right will only apply where (for example): <ul style="list-style-type: none"><li>• you dispute the accuracy of the personal information held by us</li><li>• you would have the right to ask us to delete the personal information but would prefer that our processing is restricted instead, or</li><li>• we no longer need to use the personal information to achieve the purpose we collected it for, but you need the data for the purposes of establishing, exercising or defending legal claims.</li></ul>
<b>To data portability</b>	In certain circumstances, a right to receive the personal information you have given us, in a structured, commonly used and machine-readable format. You also have the right to require us to transfer this personal information to another organisation, at your request.
<b>To object to processing</b>	A right to object to our processing of the personal information we hold about you where our lawful basis is for the purpose of our legitimate interests, unless we are able to demonstrate, on balance, legitimate grounds for continuing to process the personal information which override your rights, or which are for the establishment, exercise or defence of legal claims.

**To object to marketing** Where we process your data for marketing purposes you can object to such processing.

**In relation to automated decision making and profiling** A right for you not to be subject to a decision based solely on an automated process, including profiling, which produces legal effects concerning you, or similarly significantly affect you, for example, through points scoring, where a computer decides on the relevance of an application for a new role.

**To withdraw** A right to withdraw your consent, at any time, where we are relying on it to use your personal information (for example, to provide you with brochures and newsletters).

12.1 If you would like to contact us with any queries or comments, request further information or exercise any of your available rights set out above, please email: [data.privacy@rolls-royce.com](mailto:data.privacy@rolls-royce.com).

12.2 If you want to request a copy of your personal data please be as specific as you can about the information you want, and, if it isn't obvious (for example if you are not a current employee), explain why you expect us to hold your personal data.

### 13. **How to make a complaint**

13.1 If you are dissatisfied with the way we have handled your personal data, and want to make a complaint, please write to the Chief Privacy Officer at [data.privacy@rolls-royce.com](mailto:data.privacy@rolls-royce.com).

13.2 We will acknowledge your complaint within five working days and send you a full response within 20 working days. If we cannot respond fully in this time, we will write and let you know why, and tell you when you should get a full response.

13.3 We encourage you to contact us first if you have any queries, comments or concerns about the way we handle your personal data. If you are not satisfied with our handling of any request by you in relation to your rights or concerns, you also have the right to make a complaint to the relevant supervisory authority.