Data Privacy Policy

* * *

ITP Aero is part of the Rolls-Royce group of companies and is subject to the same standards of behaviour as the rest of Rolls-Royce. ITP Aero has adopted this Policy based on the equivalent Rolls-Royce Group Policy. This Policy is mandatory and applies to all employees and workers of ITP Aero, including the parent company and all its subsidiaries. This Policy sets the minimum standard that must be followed. Where local laws, regulations or rules impose a higher standard, that higher standard must be followed.

* * *

Introduction

As a responsible company we know it is important that we protect your personal information. Whether you are an employee, external worker, customer, supplier or other third party, such as a visitor to our sites – we will always aim to collect and process your Personal data in line with legal requirements, best practice and individual expectations.

This Policy will help us in that commitment. Data privacy laws and regulations differ depending on the country you are operating in; this Policy provides a consistent, minimum standard of working and helps us to ensure we are globally compliant. Our Policy also demonstrates to the regulators that we consider good handling of Personal data a key business principle and an integral part of our Code of Conduct.

Any breaches of this Policy could have serious consequences for us: damage to our reputation; financial penalties and limitations on our ability to use Personal data. Breaches could also result in criminal sanctions for you and your management team. It is therefore critical we all read and follow this Policy - including our contractors, subcontractors and colleagues employed in joint ventures where we have a majority share.

This Policy is mandatory and applies to all employees of ITP Aero and its subsidiaries ("ITP Aero" or "Company" or "employees"). This Policy sets the minimum standard that must be followed. Where local laws, regulations or rules impose a higher standard, that higher standard must be followed. Breaches of the ABC Policies, including this Policy, are not acceptable and may result in disciplinary action up to and including dismissal.

Our Policy explains our approach to handling Personal data, and covers the following areas:

- the minimum standards to be adopted;
- our responsibilities;
- your responsibilities;
- your rights under Data privacy legislation;
- our approach to using third parties to process Personal data.

Your responsibility

To read, understand and comply with this policy;

Raise any questions or concerns you might have. There is advice on how you can do so in Section 2.

Your manager's responsibility

To understand this policy and make sure that they do not ask you to work in a way that contravenes it.

Common terms

Personal data

Any information about living individuals, which is held in electronic form (e.g. on a computer database), or in a structured manual (paper) filing system.

Sensitive personal data

Certain types of personal data classes, laid down in legislation: racial or ethnic origin; political opinions; religious or other similar beliefs; trade union membership; physical or mental health; sexual life and/ or criminal records.

Data Privacy

The function described in section 1.4 below, aimed to protect from mishandling the personal data and information held by the Company and relating to any individual having a relation with ITP Aero.

Local country policies

A localised version of this data privacy policy, which includes country specific rights and/or obligations.

Processing

Any activity involving personal data such as collection; use; manipulation; recording; storage; retrieval; adaptation; alteration; disclosure by transmission or otherwise; dissemination; destruction or erasure.

Company

This means any company within the *ITP Aero* group, including the parent company (*Industria de Turbo Propulsores S.A.U.*), and its wholly owned subsidiaries, or any other company in which they have a controlling and/or majority shareholding.

ITP Aero

This means, as applicable, either the whole *ITP Aero* group or any Company thereof as defined above.

1.1. Legal requirements

Data privacy legislation strikes a balance between our need to collect, hold, use and disclose Personal data - and your rights and privacy expectations as an individual. Data privacy legislation means we will be held to account if we mishandle your personal information.

Data privacy legislation is not the same in every country - although there is some common ground in Europe. It is these standards set out in the European Union (EU) legislation that we use as a baseline. Please note however that we may have supporting local policies in your region where there is a unique legislative requirement which is not covered by the EU baseline.

In some countries there are serious consequences, including criminal sanctions, both for individuals and companies who breach data privacy laws. So we have decided that:

- each legal entity within our group will be responsible for the Personal data which it collects, uses, processes, or has processed on its behalf (e.g. by a third party supplier).
- it is your responsibility to uphold the principles of data privacy in the business and follow all laws and proper procedures. We may decide to take disciplinary action if you do not.
- contractors (individual or corporate) should behave like employees when processing Personal data, except where we specify otherwise in their contract terms.
- Data privacy requirements should not be viewed in isolation. Other laws – and associated risks – will also apply when handling Personal data. For example human rights legislation; the common law of confidentiality.

1.2. Processing of Personal data

1.2.1. Personal data

Personal data is any information about living, identifiable individuals. This can be information which relates to either someone's professional or private life. It includes basic data such as name or contact details, as well as more sensitive types of data such as racial origin; criminal convictions, or medical data. We collect and use Personal data in both paper and electronic form.

1.2.2. ITP Aero and Personal data

We need to collect, use and often transfer Personal data around the organisation for business reasons and to benefit various groups of people, including, but not limited to:

- prospective, current and ex-employees
- sub-contractors and external workers
- suppliers of goods / services
- clients and customers
- visitors to our sites.

1.2.3. Processing of employees' Personal data

We will use your Personal data, and information obtained from other sources, for, but not limited to:

- personnel administration such as recruitment; employee performance management and professional development
- management purposes such as scheduling
- payroll and pensions administration
- travel management
- building and managing external relationships such as with suppliers and customers
- purposes required by law or regulation such as equal opportunities monitoring.

We aim to make sure that Personal data held about you is accurate and up to date, both whilst you are working for us and after. It is your responsibility to notify us straight away if there are any changes in your personal circumstances so that we can keep your information updated.

1.2.4. Processing of non-employees' Personal data

We often process Personal data about individuals other than employees - such as customer contacts, visitors to sites, suppliers, website users and shareholders. We do this for a number of reasons, including:

- share plan management and operations
- health and safety purposes
- visitor management
- business and market development
- building and managing external relationships
- planning and delivery of goods and services
- research and development
- knowledge management
- training
- other purposes required by law or regulation.

Important note: We collect and, process and use all Personal data to the same high standards, regardless of whose data it is. Therefore we should all handle non-employee data with exactly the same care as employee data.

1.2.5. Processing of Sensitive personal data

Sensitive personal data is defined under the EU legislation as racial or ethnic origin; political opinions; religious or other similar beliefs; trade union membership; physical or mental health; sexual life and/ or criminal records. We work to this definition, and will not collect this type of information unless:

- you agree that we may do so, based on a full understanding of why the data is being collected, e.g. in order to process pre-employment checks. In exceptional circumstances we may rely on consent given on your behalf, for example, by a family member, or

- we need to do so to meet our obligations or exercise our rights under employment law e.g. for reporting on ethnicity, or
- in exceptional circumstances such as where the processing is necessary to protect your vital interests e.g. you need access to specific drugs to ensure your health, or
- in circumstances permitted by data privacy laws. For example in countries where background checks play a more prominent role. This does not mean however that we can collect sensitive data without appropriate judgment. We always need to decide, and be able to justify, how necessary it is to collect this information, and if there is any alternative to doing so.

1.2.6. Monitoring of Personal data

There may be situations where, for quality control, training, security and/or investigation purposes, we monitor recordings of your telephone, internet access/ usage and email communications. This is explained in more detail in our IT policies.

1.3. Our responsibilities

We are committed to complying with data privacy legislation in all the countries we operate in when processing your data. To demonstrate this commitment we will ensure that:

- there is someone designated as having specific responsibility for data privacy in each legal entity
- there is a full-time Data Privacy lead and dedicated local/ national leads throughout our Company, who will be fully supported by our senior management team
- we monitor changes in Data privacy legislation and implement these as appropriate
- everyone managing and handling Personal data understands that they are responsible for following good Data privacy practice
- everyone managing and handling Personal data is appropriately trained and adequately supervised
- anyone with a question about handling Personal data knows where to go for advice and is supported in knowing what to do
- queries about handling Personal data are promptly, professionally and courteously dealt with
- processes for handling Personal data are clearly described in policies and procedures to ensure excessive data is not collected; data is not stored for longer than necessary; confidentiality and security is respected at all times
- methods, such as collection and destruction, of handling Personal data are regularly reviewed
- any data handling breaches are logged, fully investigated, and reported to the appropriate regulatory authority where necessary.

The following sections are aligned to the privacy principles, and set out our specific

commitments to demonstrate compliance with legislation.

Important note: Our business area leaders have overarching responsibility for ensuring our Data privacy standards are followed in their particular business area.

1.3.1. Fair and lawful processing

It is our duty to process Personal data fairly and lawfully, so we will only process Personal data if:

- you have consented to the processing (where consent is necessary), or
- we need to carry out such processing to enter into a contract with you, or
- we need to comply with a legal obligation, or
- we need to protect your vital interests in a 'life or death' situation, or
- we need to process the data to pursue our legitimate interests, and those interests are not overridden by your interests, rights or freedoms, or
- for any other purpose permissible under relevant privacy laws.

In addition we will:

- make sure that you know the identity of the specific company collecting/ using the data if it is not obvious (e.g. if a third party is collecting data on our behalf)
- make sure you are made aware of how your Personal data is processed when it is first collected, or as soon as possible afterwards
- make sure that if Personal data has already been collected and processed and it is then going to be used in a new way or for different purposes, or where the data is collected from a new third party, we will inform you of the change.

We will do all of this in various ways, for example: explanations in terms of employment; sections in the employee handbook; guidance on webpages; during training sessions.

1.3.2. Accuracy of data

It is our responsibility to have procedures and systems in place to ensure that:

- we do not collect excessive Personal data
- Personal data is adequate, relevant, accurate and up to date for the intended purposes
- we process Personal data only for the purposes specified in this policy, associated local policies or in information provided to you.

1.3.3. Retention and destruction of data

We will maintain retention policies and procedures so that your Personal data is destroyed after an appropriate amount of time given the purposes for which the data is used - except where another law requires us to keep the data for a certain length of time. When we do delete your data, we will make sure we do it in a secure and confidential way.

1.3.4. Security of data

We will maintain organisational, physical and technical security arrangements in relation to the Personal data we hold. We will ensure that those arrangements are appropriate to the risks represented by the processing of and the nature of the Personal data. Where appropriate these arrangements will include provisions for 'need to know' access to Personal data.

We will ensure that appropriate diligence activities are carried out in relation to the security of Personal data, both before and after we use it and/or take responsibility for it.

1.3.5. Sharing Personal data with service providers

We often use third party suppliers to process Personal data e.g. for training management, health and safety control; recruitment purposes; medical checks and analysis; tax counsellors for expatriates.

Where this is the case we are seen as using a 'data processor' under the terms of privacy legislation, and must always put in place contractual terms to safeguard the Personal data we share with them. We have standard wording which allows us to ensure that the data processor:

- processes Personal data only on our instructions
- has appropriate technical and organisational security measures
- makes all reasonable efforts to maintain Personal data so that they are accurate and up to date at all times
- does not keep the Personal data for longer than they are our service providers, or are permitted by the terms of the agreement
- does not disclose the Personal data to any person except as required or permitted by law, the agreement, or with our written consent
- provides full co-operation and assistance to us in allowing you to exercise any right under this policy and applicable legislation
- agrees that we may monitor the data processing, including visits to undertake compliance auditing and investigating any reported breaches
- ensures that any sub-contractor they use also follows our standards.

Personal data also needs to be treated with particular care in countries which do not have data privacy laws, or whose laws do not provide a level of protection equivalent to the standard within the EU. Therefore we will not transfer Personal data to other companies for processing unless they agree to abide by a Data privacy standard at least as high as this policy; or enter into a contractual arrangement which includes the approved EU standard clauses for transfers of Personal data outside of the EU. Our responsibilities extend to the sub-contractor level, so it is important to ensure that appropriate contractual controls are always in place to minimise our risks. The only exceptions are where:

- the transfer is necessary to protect your vital interests in a 'life or death' situation

- to enter into or perform a contract with you (or for your benefit)
- you have consented to the transfer.

1.4. Data Privacy function

The Data Privacy function is responsible for the following:

- setting of strategy, provision of policy and compliance processes
- monitoring Data privacy legislation and advising on Data privacy risks and mitigating actions
- auditing throughout our Company and third party service providers to assess Data privacy compliance levels
- assessing risks to both us and you from data breaches and advising on remedial actions
- training and awareness
- ensuring that we deal with requests for access to Personal data in line with legislative requirements
- notification and communication with the appropriate regulatory authority.
- you have consented to the transfer.

1.5. Your responsibilities

It is the responsibility of all of us to make sure that our Company complies with all Data privacy laws. Whenever Personal data is collected or used in any way, the principles set out in this Policy, and any associated documents, must be followed by those of us handling the Personal data. We have created seven key privacy messages, based on legislative requirements, in section 1.6 which everyone in our business must follow when processing Personal data.

To help us maintain a level of awareness around our responsibilities, on-line training; is available from the Data Privacy function, or local Data privacy contacts.

There are a number of areas of the business that have key responsibilities for handling and processing Personal data (e.g. Human Resources), and specific procedures, guidelines, and training will be made available for such areas.

In some countries certain breaches of Data privacy legislation can lead to personal criminal liability for you as well as us. Failure of employees to comply with their responsibilities under this Policy and any associated procedures or guidelines may be deemed as misconduct and result in disciplinary action.

1.6. Seven key privacy messages for our employees

Good Data privacy compliance can be summarised into seven key controls. Please make sure you understand and apply them whenever you are handling Personal data:

1. Notice and transparency – we need to tell individuals if we are processing information about them. We need to explain what information we are using, why we need it and what we will do with it.

2. Purpose and choice – once we have collected the data we will only use it for the

specific purpose we have promised. If we need to use it for another purpose, we will go back to tell the individual and ask for any necessary permission.

3. Quality – Personal data must be accurate and kept up to date. The data must be relevant to the reason we are collecting and processing it – and we need to make sure we do not collect information we do not need.

4. Security – we must take appropriate steps to protect the Personal data we hold. We do not want it getting into the wrong hands, or even lost. Things to consider when thinking about security measures are the nature of the data and the potential effects of losing it. We will need to make sure our third parties do the same.

5. Transfer – some countries restrict the transfer of Personal data depending on where you are moving the data is going to and what safeguards are in place in that new location. You will need to check if restrictions apply, and if so, whether any control mechanisms are in place (such as inter-group agreements between the transferring and receiving companies).

6. Retention – we must only keep Personal data for as long as we need it (and in relation to the purpose we collected it). Retention policies must be followed and data destroyed properly.

7. Access and rectification – if an individual requests access to their data we need to provide this. Often legislation means we are required to do this in a time-limit too. We will also need to change any factually incorrect data where requested.

1.7. Individuals' rights

It is important that you understand your individual rights when it comes to Data privacy. This section highlights certain rights we all have, whether we are employees or not, in relation to our Personal data.

It is possible that these rights may be increased, or slightly different under local data privacy legislation. Our local country Data privacy policy will therefore set out all such rights in detail.

1.7.1. Right of access

In certain countries you will have the right to ask for a copy of the Personal data held about you, and for any inaccuracies in the information to be corrected.

We will process these requests, whether they are received from yourself, other individuals or third parties acting on your behalf - such as solicitors. The actual steps within the process may differ depending on the region you are in, so to exercise this right you should go to the local Data privacy contact or the local HR representative for information.

1.7.2. Right of correction

Anyone may ask that we correct the Personal data we hold about them. If we agree that the data is incorrect, we will delete or correct the data. If we do not agree that the data is incorrect, we will note within the relevant record the fact that you consider the data to be incorrect.

1.7.3. Right to object to direct marketing

We will abide by any request from you not to use your Personal data for direct marketing purposes.

1.7.4. Rights in relation to automated decision taking

We will not generally make any decisions that significantly affect you (e.g. performance at work; reliability; conduct) solely on the basis of automatic processing of the data we hold. Where we do use such decision making techniques, we will make sure that we put measures in place to check our decisions are fair and you are given an opportunity to discuss them

1.7.5. Right to object to processing for compelling reasons

You may want us to stop processing your Personal data for various reasons. If you do, and we think the reason is compelling and legitimate we will discuss the possibility of stopping the processing of your data straight away with you.

1.8. Governance

We will make sure that we:

- facilitate compliance with our Policy
- allow you to exercise your Data privacy rights
- listen, consider and respond to any complaints that this policy has not been followed.

If you want to exercise your Data privacy rights, or need assistance with any of the actions outlined in this policy, please contact your local Data privacy contact or the Data Privacy function.

Important note: If you do not know who your local Data privacy contact is, you can email the Data privacy team (dataprivacy@itpaero.com).

It is important you remember that any breach of this Policy (or the policies referred to within it) may, following an investigation, result in disciplinary action potentially up to and including dismissal.

1 Governing our policy

2.1 Roles and responsibilities

Who	Responsible for
You	• reading, understanding and following our Policy; understanding your individual rights with regards to data privacy. • applying the seven key Data privacy controls (section 1.6) whenever you manage or handle Personal data. • reporting any breaches, or suspected breaches, of this Policy to your local Data privacy lead, or the Data Privacy function, immediately.
Senior leaders includes Sector Presidents and the Executive team	• ensuring the Company's Data privacy standards (as outlined in this policy) are upheld and monitored within their business area. • ensuring there is someone designated as having specific responsibility for Data privacy in their legal entity, to work closely with the Data Privacy function, and local / national leads in their business area; and ensuring full senior management support for Data privacy leads in their business area. • ensuring that everyone in their business area who manages or handles Personal data is suitably trained and supervised. • making clear, within their business area, where employees with questions on any aspect of Data privacy, should go for advice.
Data Privacy function	• setting of strategy, provision of policy and compliance processes. • monitoring Data privacy legislation and advising on Data privacy risks and mitigating actions. • auditing throughout our Company and third party service providers to assess Data privacy compliance levels. • assessing risks to both us and you from data breaches and advising on remedial actions. • training and awareness. • ensuring that we deal with requests for access to Personal data in line with legislative requirements. • notification and communication with the appropriate regulatory authority.
Local data privacy leads	• liaising with the Data Privacy function on implementing and maintaining privacy control measures. Maintaining regular reports to the Data Privacy function. • ensuring queries about Personal data are promptly, professionally, and courteously dealt with. • reviewing methods, such as collection and destruction, of handling Personal data regularly and escalating any risks identified to the Data Privacy function. • advising business area management teams of changes in Data privacy legislation, and supporting changes in Data privacy practice as appropriate. • ensuring any data handling breaches are reported to the Data Privacy function, and supporting in any investigatory action as necessary.

2 Where to find out more

If you have any questions or need further information, you can contact:

- Name: Alberto Aller de la Fuente
  Role: ITP Aero Information Compliance Management Manager
  Address: Industria de Turbo Propulsores S.A., Francisca Delgado, 9, 28108, Alcobendas, Madrid
  Telephone: +34 912 079 448
  Mobile: +34 645 214 910
  Email: alberto.aller@itpaero.com

- Name: Manuel P. González San Segundo
  Role: ITP Aero Executive Director of Organization & Resources
  Address: Industria de Turbo Propulsores S.A., Francisca Delgado, 9, 28108, Alcobendas, Madrid
  Telephone: +34 912 060 144
  Mobile: +34 607 428 158
  Email: manuel.gonzalez@itpaero.com

- The ITP Aero Ethics Line

  Available at the intranet ecm.itpaero.com and the website www.itpaero.com

3 Other documents you should read

- The *ITP Aero* Code of Conduct
- The ABC Policies and guidance documents on the *ITP Aero* intranet Ethics & Compliance site
- The *ITP Aero* IT Acceptable Use Policy