DATA PROTECTION AT LEONARDO UK

Privacy Notice for Employees and Contract Staff – Past, Present and Prospective

Protecting and keeping your personal information secure

What is the purpose of this document?

Leonardo UK Ltd (the "Company", "we", or "us") is committed to protecting the privacy and security of the personal information we hold about employees and contract staff, past, present and prospective (collectively, "Staff"). This Privacy Notice explains how we collect, use and share personal information about you before, during and after your working relationship with us, in accordance with the UK General Data Protection Regulation (UK GDPR) and the UK Data Protection Act 2018 (as amended) (together, "Data Protection Law").

For the purposes of Data Protection Law, the Company is the "Data Controller". This means we determine the purposes and means of processing your personal information and are responsible for it. We are required by law to provide you with the information contained in this Privacy Notice.

This notice applies to prospective, current and former employees and contract staff. It does not form part of any employment contract or any other contract for services. We may update this notice from time to time and will notify you of any significant changes.

This is the overarching Privacy Notice in relation to your work with us. In the interests of transparency, we may also issue additional notices for particular processing activities where appropriate.

Data Protection Principles

We will comply with Data Protection Law. The personal information we hold about you must be:

1. Used lawfully, fairly and in a transparent manner;

2. Collected only for valid purposes that we have clearly explained to you, and not used in ways that are incompatible with those purposes;

3. Relevant to the purposes we have told you about and limited to what is necessary;

4. Accurate and, where necessary, kept up to date;

5. Kept only for as long as necessary for the purposes we have explained;

6. Kept securely; and

7. Managed in an accountable manner.

The kind of information we hold about you

Personal data (or personal information) means any information about an individual from which that person can be identified. It does not include data where the identity has been removed (anonymous data). Some personal data is more sensitive and requires a higher level of protection ("Special Categories"), such as information about health or ethnicity.

At any time during your working relationship with the Company, we may collect, store and use some or all of the following categories of personal information about you:

- Personal contact details (name, title, addresses, telephone numbers, personal email addresses);
- Date of birth;
- Gender;
- Marital status and dependants;
- Next of kin and emergency contact information;
- National Insurance number;
- Nationality;
- Bank account details, payroll records and tax status information;
- Salary, annual leave, pension and benefits information;
- Start date;
- Location of employment or workplace;
- Copy of driving licence;
- Copy of passport;
- Recruitment information (including copies of right-to-work documentation, references and other information included in a CV or cover letter or as part of the application process);
- Employment records (including job titles, work history, working hours, training records and professional memberships);
- Compensation history;
- Performance information;
- Disciplinary and grievance information;
- CCTV footage and information obtained through electronic means (e.g. swipe card records);
- Information about your use of our information and communications systems;
- Work mobile phone usage records;
- Photographs;
- Safety-related records (e.g. incident reports).

We may also collect, store and use the following Special Categories of more sensitive personal information:

- Information about your race or ethnicity;
- Trade union membership;

- Information about your health, including any medical condition, health and sickness records;
- Information about criminal convictions and offences.

How is your information collected?

We collect personal information about Staff through the application and recruitment process, either directly from candidates or from employment agencies and background-check providers. We may collect additional information from third parties such as former employers, credit reference agencies or other background-check providers. Given the nature of our business, both the Company and Staff are required to comply with the National Security Act 2023 and the Official Secrets Act 1989, which may involve enhanced security checks.

We also collect additional personal information in the course of job-related activities during your work with us.

How we will use information about you

We will only use your personal (including Special Category) information when the law allows us to. Most commonly we will use it:

- Where we need to perform the contract we have entered into with you;
- Where we need to comply with a legal obligation; and
- Where it is necessary for our legitimate interests (or those of a third party) and your interests and fundamental rights do not override those interests.

We may also use your information in the following, less common, situations:

- Where we need to protect your vital interests (or those of another person);
- Where it is needed in the public interest or for official purposes; and
- Where we are required to co-operate with a regulatory or investigatory body.

For Occupational Health activities we may need to process Special Category data for the purposes of preventive or occupational medicine, assessing working capacity, medical diagnosis, the provision of health or social care or treatment, or the management of health or social care systems and services. Such processing is subject to conditions and safeguards, including professional confidentiality obligations.

Situations in which we will use your information

From time to time we may use any or all of the categories of information listed above. This enables us to perform our contract with you (or with your employer if you are a contractor), support your safety and wellbeing, and comply with legal obligations. In some cases we may rely on our legitimate interests (or those of a third party) following an appropriate balancing assessment.

- Making decisions about your recruitment or appointment;
- Determining the terms on which you work for us;

- Checking you are legally entitled to work in the UK;
- Enabling and maintaining security clearances;
- Paying you and, if you are an employee, deducting tax and National Insurance contributions;
- Providing employment benefits (e.g. private healthcare);
- Liaising with your pension provider;
- Administering the employment/contractor contract we have entered into with you;
- Business management and planning, including accounting and auditing;
- Conducting performance reviews, managing performance and determining performance requirements;
- Making decisions about salary reviews and compensation;
- Assessing qualifications for a particular job or task, including decisions about promotions;
- Gathering evidence for possible grievance or disciplinary hearings;
- Making decisions about your continued employment or engagement;
- Making arrangements for the termination of our working relationship;
- Education, training and development requirements;
- Dealing with legal disputes involving you or other Staff, including accidents at work;
- Ascertaining your fitness to work;
- Managing sickness absence;
- Complying with health and safety obligations;
- Preventing fraud;
- Monitoring your use of our information and communications systems to ensure compliance with our IT and Security policies;
- Ensuring network and information security, including preventing unauthorised access to our systems and preventing malicious software distribution;
- Conducting data analytics studies to review and better understand Staff retention and attrition rates;
- Equal opportunities monitoring;
- Supporting bid activities (e.g. submitting work CVs as part of bid documentation);
- Assisting customers to identify relevant employees for security purposes; and
- Making visa applications for working overseas.

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

If you fail to provide information

If you fail to provide certain information when requested, we may not be able to perform the contract we have (or would) enter into with you (for example, paying you or providing a benefit), or we may be prevented from complying with our legal obligations (for example, to ensure the health and safety of our workers).

Change of purpose

We will only use your personal information for the purposes for which we collected it, unless we reasonably consider that we need to use it for another purpose and that purpose is compatible with the original purpose. If we need to use your personal information for an unrelated purpose, we will notify you and explain the legal basis that allows us to do so.

We may process your personal information without your knowledge or consent where this is required or permitted by law.

How we use particularly sensitive information

Special Categories of personal information require higher levels of protection. We have in place an appropriate policy document and safeguards that we are required by law to maintain. We may process Special Category data in the following circumstances:

- In limited circumstances, with your explicit prior written consent;
- Where we need to carry out our legal obligations or exercise rights in connection with employment; and
- Where it is needed in the public interest, such as equal opportunities monitoring or in relation to our occupational pension scheme.

More rarely, we may process such information where it is needed in relation to legal claims, where it is necessary to protect your vital interests (or those of another person) and you are not capable of giving consent (for example, if you are taken ill overseas on business), or where you have already made the information public. We may also process such information in the course of legitimate business activities with appropriate safeguards.

Our obligations as an employer

We may use your particularly sensitive personal information in the following ways:

- Information relating to leaves of absence (including sickness absence or family-related leaves) to comply with employment and other laws;
- Information about your physical or mental health, or disability status, to ensure your health and safety in the workplace, assess your fitness to work, provide appropriate workplace adjustments, monitor and manage sickness absence and administer benefits;
- Information about your race, nationality or ethnic origin to ensure meaningful equal-opportunity monitoring and reporting; and
- Trade union membership information to pay trade union premiums, register protected employee status and comply with employment law obligations.

Do we need your consent?

We do not need your consent if we process Special Category personal information in accordance with our written policy to carry out our legal obligations or to exercise

specific rights in the field of employment. In limited circumstances we may ask for your written consent to process certain particularly sensitive data. If we do, we will provide full details so that you can consider whether you wish to consent. It is not a condition of your contract with us that you agree to any such request.

Information about criminal convictions

We may only use information relating to criminal convictions where the law allows us to do so. This will usually be where such processing is necessary to carry out our legal or security obligations (e.g. security vetting) and provided we do so in line with our data protection and security policies.

More rarely, we may use information relating to criminal convictions where it is necessary in relation to legal claims, to protect your vital interests (or those of another person) where you are unable to give consent, or where you have already made the information public. We do not envisage holding criminal-convictions information as a matter of course, but we may need to do so from time to time to meet security obligations.

We will only collect information about criminal convictions where appropriate for the role and where we are legally permitted to do so. Where appropriate, we will collect such information as part of the recruitment process, or you may notify us during your engagement. Verification of any unspent convictions under the Rehabilitation of Offenders Act 1974 may be retained for the purpose of completing Baseline Personnel Security Standard (BPSS) clearance.

We are permitted to process such information to carry out our obligations under the Official Secrets Act 1989. We maintain appropriate policies and safeguards, including technical and organisational measures (such as encryption) and restricted access by dedicated individuals.

Automated Decision-Making

Automated decision-making occurs when an electronic system uses personal information to make a decision without human intervention. We may only use automated decision-making in the following circumstances:

- Where we have notified you of the decision and given you 21 days to request human reconsideration;
- Where it is necessary to perform the contract with you and appropriate measures are in place to safeguard your rights; or
- In limited circumstances, with your explicit written consent and with appropriate safeguards.

If we make an automated decision based on Special Category personal information, we must have your explicit written consent or a justification in the public interest, and we will put in place appropriate measures to safeguard your rights. You will not be subject to

decisions that have a significant effect on you based solely on automated processing unless we have a lawful basis and have notified you.

We do not currently envisage taking decisions about you using automated means. We will notify you in writing if this changes.

Data Sharing

We may need to share your personal information with third parties, including service providers and other entities in the Leonardo group. We require third parties to respect the security of your data and to process it in accordance with the law. We may transfer your information outside the UK/EEA (for example, to other companies in the Leonardo group or to service providers). If we do, we will ensure an appropriate level of protection.

Why might you share my personal information with third parties?

We will share your personal information with third parties where required by law, where it is necessary to administer the working relationship with you, or where we have another legitimate interest in doing so (for example, in connection with the sale and purchase of goods and services or administering overseas contracts).

Which third-party service providers process my personal information?

"Third parties" include service providers (including contractors and designated agents) and other entities within our group. Typical activities include payroll, pension administration, benefits provision and administration, IT services, travel and expenses, and company credit cards. Key suppliers include:

- Accenture – Finance;
- Aetna – International Health Care;
- AIG – Reward;
- American Express (AMEX) – Expenses;
- AON – Employee Benefits;
- Avis – Car Rental;
- Aviva Care First – Employee Assistance Programme;
- Bupa – Health Care;
- Carlson Wagonlit Travel – Travel;
- Concur – Travel & Expenses;
- Coursera (USA) – Training and development activities;
- DXC (formerly Xchanging) – Contract recruitment, indirect procurement and IT infrastructure;
- EQA – Apprenticeship management;
- Hyland (formerly Kofax) – Employee files;
- iJET – Travel security risk management;
- Insight Skills – Apprenticeship management;
- Iron Mountain – Storage of documentation;

- NGA HR – Apprenticeships, payroll, employment contracts/files, travel, recruitment & reward;
- Outposts – Apprenticeship management;
- Personal Group – Voluntary benefits;
- Tribal – Apprenticeship management;
- Unite – Trade Union;
- Viva Glint – for employee surveys
- Warwick – Apprenticeship management;
- XPS Administration – Pensions administration;
- Willis Ltd - Travel
- Zellis – Apprenticeships, payroll, employment contracts/files, travel, recruitment & reward.
- Zurich – Employee travel insurance;

IT at Leonardo UK also shares data with our parent company, Leonardo S.p.A., as part of Security and HR activities, and for shared IT functions (e.g. email servers).

How secure is my information with third-party service providers and other entities in Leonardo's group?

All third-party service providers and other group entities are required to take appropriate security measures to protect your personal information in line with our policies, which are reviewed by the Security function. We do not allow third-party service providers to use your personal data for their own purposes and only permit them to process it for specified purposes in accordance with our instructions. Each processor undergoes a proportionate risk assessment to determine the adequacy of its technical and organisational security measures.

When might you share my personal information with other entities in the Leonardo group?

We may share your personal information with other group entities as part of regular reporting on company performance, in the context of business reorganisation or group restructuring, for system maintenance support and hosting of data, and otherwise only for purposes consistent with this notice.

What about other third parties?

We may share your personal information with other third parties, for example in connection with a possible sale or restructuring of the business. We may also need to share your information with a regulator or to comply with the law.

Transferring information outside the UK/EEA

We may transfer personal information to countries outside the UK/EEA, including the United States and India, to perform our contract with you. These countries may not be subject to an adequacy decision, meaning they are not deemed to provide an equivalent level of data protection. Where such transfers occur, we will ensure appropriate

safeguards are in place, such as the use of Standard Contractual Clauses, to protect your information.

Where your personal data needs to be exported in support of bid and/or commercial activity with an overseas customer or supplier, this will be done in consultation with you to ensure that only the minimum necessary personal information is disclosed and your rights are protected. A typical example is a sanitised work CV containing experience and qualifications. In such cases, the basis for transfer is compelling legitimate interests.

Data Security

We have implemented appropriate technical and organisational measures to protect your personal information. Details of these measures are available to employees on request from Leonardo.SAR@leonardocompany.com. Third parties will process your personal information only on our instructions and where they have agreed to treat it confidentially and keep it secure.

We limit access to your personal information to those employees, agents, contractors and other third parties who have a business need to know. They will only process your personal information on our instructions and are subject to a duty of confidentiality. We have procedures in place to deal with any suspected data security breach and will notify you and any applicable regulator where legally required.

Data Retention

How long will we use your information for?

We will retain your personal information only for as long as necessary to fulfil the purposes for which it was collected, including satisfying any legal, accounting or reporting requirements. Details of retention periods for different categories of personal information are set out in our retention policy on the Company intranet. We consider the amount, nature and sensitivity of the data, the potential risk of harm from unauthorised use or disclosure, the purposes for which we process it and whether those purposes can be achieved by other means, and applicable legal requirements.

In some circumstances we may anonymise your personal information so that it can no longer be associated with you; in that case, we may use such information without further notice. Once you are no longer an employee or contract staff member, we will retain and securely destroy your personal information in accordance with our data retention policy.

For unsuccessful job applicants, personal data provided during the application process will be retained for a maximum of 12 months, to allow us to notify you of other suitable opportunities, after which it will be permanently deleted. A copy of the Company’s Data Retention Policy is available on request from Leonardo.SAR@leonardocompany.com.

Rights of Access, Correction, Erasure and Restriction

Your duty to inform us of changes

It is important that the personal information we hold about you is accurate and current. Please keep us informed of any changes (for example, address or marital status) during your working relationship with us.

Your rights in connection with personal information

Under certain circumstances, you have the right to:

- Request access to your personal information (a "data subject access request");
- Request correction of the personal information that we hold about you;
- Request erasure of your personal information where there is no good reason for us to continue processing it;
- Object to processing where we rely on legitimate interests and your particular situation gives you grounds to object; you also have the right to object to processing for direct marketing;
- Request restriction of processing of your personal information (for example, to establish its accuracy or the reason for processing);
- Request the transfer of your personal information to another party; and
- Be informed if we permit or become aware that a third party has shared your data in a way that does not conform to the purposes outlined in this notice.

If you wish to exercise any of these rights, please contact the Company's Data Protection Management Team at Leonardo.SAR@leonardocompany.com.

No fee usually required

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

What we may need from you

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

Right to withdraw consent

In the limited circumstances where you have provided your consent to the collection, processing or transfer of your personal information for a specific purpose, you have the right to withdraw your consent for that specific processing at any time. To withdraw consent, please contact the Company's Data Protection Management Team at Leonardo.SAR@leonardo.com or your HR representative. Once we have been notified of your withdrawal, we will no longer process your information for the purpose(s) you originally agreed to, unless we have another lawful basis to do so.

Use of employees/contractors in developing and testing products and services

Leonardo has a legitimate interest in supporting the testing, development and demonstration of its products and services. To achieve this, we may occasionally need to include limited personal data of employees/contractors to support these activities. For example, if we are developing a camera to feed a facial recognition system, we may need to capture images of real people to test the system.

It is also possible, in very limited circumstances, that personal data belonging to members of the public may be subject to *incidental capture*. This occurs where the nature of testing makes the collection of such data unavoidable. For example, if an airborne camera is tested over a populated area, images of individuals on the ground may be recorded. Any incidental capture is handled with strict sensitivity and security, and no such data will be published unless it has first been anonymised, for example through pixelation.

Any and all such activity is subject to careful consideration of data protection matters. Each project will include an analysis of risks, control measures and communications to affected individuals to ensure rights are respected in accordance with company protocols. No such testing will be conducted without impacted individuals being informed in advance and given the opportunity to object. Project-specific privacy notices may be provided where necessary.

The kind of information we may hold includes images, voice recordings and technical identifiers (e.g. IP address, vehicle registration mark or asset serial number). It is very unlikely that Special Category information would be captured; if it were, a specific arrangement would be put in place and communicated in advance.

Information may be collected using systems engineered or under test by Leonardo as part of our business of providing products and solutions to customers.

We use this information to enable testing, development and demonstration of Leonardo products and customer solutions where interactions with natural persons are inherent to the operation. The lawful basis will typically be our legitimate interests in developing new products or to satisfy a contractual need. In some circumstances we may need to use the information to protect your or someone else’s vital interests, particularly safety. Although the information is real, it is used in a simulated environment, which significantly reduces the risk of adverse impact (for example, testing an artificial credit-scoring system using your data would not affect your real-world credit score).

We will only use real data where it is impractical to use simulated/synthetic or pseudonymised/anonymised data.

We will only use particularly sensitive information in specific circumstances with suitable arrangements in place and clear advance communication to affected individuals.

Data Protection Management Team

The Company has established a dedicated Data Protection Management Team (DPMT) responsible for overseeing day-to-day data protection matters. This function brings together specialist expertise from the Data Governance, Cybersecurity, Legal and HR teams. The Data Protection Management Team reports to the Data, Knowledge and Information Committee, which meets quarterly and in turn reports directly to the CEO.

Processing of Under-18s' Personal Data

The Company may occasionally process the personal data of children (individuals under 18 years of age). Examples include:

- Bring-a-child-to-work days;
- STEM activities or school engagements;
- Work experience; and
- Apprenticeships (under 18).

Each such activity is carried out on the basis of the Company's legitimate interests. Given the particular requirements associated with processing children's personal data, we will engage directly with the relevant school or parent/guardian to ensure that any such processing is understood and appropriate.

In certain exceptional circumstances, the Company may be required by law to disclose information to regulatory bodies or social services. Any such disclosure will be made in full compliance with relevant laws and guidance, such as Keeping Children Safe in Education.

Changes to this Privacy Notice

We reserve the right to update this Privacy Notice at any time. We will provide you with a new notice when we make any substantial updates. We may also notify you in other ways from time to time about the processing of your personal information.

If you have any questions about this Privacy Notice, please contact the Company's Data Protection Management Team or the Data Protection Officer at Leonardo.SAR@leonardo.com.

You can also contact the Information Commissioner's Office at casework@ico.org.uk, citing our Registration Number Z6375415.

Signed

Marc Jones, VP Legal Corporate Affairs

Data Protection Officer

Leonardo UK Ltd