

## DATA PROTECTION AT LEONARDO UK

### PRIVACY NOTICE FOR EMPLOYEES AND CONTRACT STAFF

*(Issued June 2021)*

---

#### 1. What is the purpose of this document?

Leonardo UK Ltd (the **Company** or **we**) is committed to protecting the privacy and security of the personal information we hold on employees and contract staff, past, present and prospective (collectively referred to as **Staff**).

This “Privacy Notice” describes how we collect and use personal information about you, as an individual Data Subject, before, during and after your working relationship with us, in accordance with the General Data Protection Regulation (GDPR), which came into force on 25 May 2018.

The legal basis upon which we rely to hold and process your data is both the fulfilment of your contract for services as well as the legitimate interests of the Company as well as complying with Legal Requirements (such as paying tax or managing occupational health), in accordance with the GDPR.

For the purposes of the GDPR the Company is a “Data Controller”. This means that we are responsible for deciding how we hold and use personal information about you. We are required under data protection legislation to notify you of the information contained in this privacy notice.

This notice applies to prospective, current and former employees and contract staff. This notice does not form part of any contract of employment or other contract to provide services. We may update this notice at any time. However, if we do so we will issue a communication to advise you of this.

This is the overarching Privacy Notice in relation to your work with us. However, to ensure transparency and compliance we may at times issue additional notices in relation to any particular processing activity that warrants it.

#### 2. Data Protection Principles

We will comply with the GDPR and relevant data protection law. The GDPR says that the personal information we hold about you must be:

1. Used lawfully, fairly and in a transparent way.
2. Collected only for valid purposes that we have clearly explained to you and not used in any way that is incompatible with those purposes.
3. Relevant to the purposes we have told you about and limited only to those purposes.
4. Accurate and kept up to date.
5. Kept only as long as necessary for the purposes we have told you about.
6. Kept securely.
7. Managed in an accountable manner.



### 3. 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).

There are “special categories” of more sensitive personal data that require a higher level of protection, such as medical information or information relating to ethnicity.

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

- Personal contact details such as name, title, addresses, telephone numbers, and 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 other information obtained through electronic means such as swipe card records.
- Information about your use of our information and communications systems.
- Work mobile phone usage.
- Photographs.
- Safety.



We may also collect, store and use the following “special categories” of more sensitive personal information:

- Information about your race or ethnicity.
- Gender Identity.
- Trade union membership.
- Information about your health, including any medical condition, health and sickness records.
- Information about criminal convictions and offences.

#### **4. How is your information collected?**

We collect personal information, sensitive or otherwise, about Staff through the application and recruitment processes, either directly from candidates or sometimes from an employment agency or background check provider. We may sometimes collect additional information from third parties including former employers, credit reference agencies or other background check agencies. This is particularly the case at Leonardo as both the Company and Staff must comply with the Official Secrets Act 1989 in the execution of Leonardo’s business and attached to that are enhanced security checks on individuals.

We will collect additional personal information in the course of job-related activities throughout the period of you working for us.

#### **5. How we will use information about you**

We will only use your personal, or special category personal, information when the law allows us to. Most commonly, we will use your personal information in the following circumstances:

1. Where we need to perform the contract we have entered into with you.
2. Where we need to comply with a legal obligation.
3. Where we need to ensure equality of opportunity for all employees
4. 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 personal information in the following situations, which are likely to be rare:

- Where we need to protect your vital interests (or someone else’s interests).
- Where it is needed in the public interest or for official purposes.
- Where we are required to co-operate with the activities of a regulatory or investigatory body.

For Occupational Health activities we need to process your “special category data” for the “purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health”. This processing is also subject to conditions and safeguards specified by relevant nursing and medical professional bodies.



## 6. Situations in which we will use your information

From time to time we may need any or all of the categories of information listed above, primarily this allows us to perform our contract with you (or in the case of contractors, our contract with your employers), for your safety and well-being in the fulfilment of your duties and to enable us to comply with legal obligations. In some cases we may use your personal, or sensitive, information to pursue legitimate interests of our own or those of third parties, provided your interests and fundamental rights do not override those interests and the necessary balancing activity has taken place. The situations in which we will process your personal, or sensitive, information are listed below.

- 
- Making a decision 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 certain employment benefits to you, such as private healthcare.
- Liaising with your pension<sup>1</sup> provider.
- Administering the employment/contractor contract we have agreed 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.
- To prevent fraud.
- To monitor your use of our information and communication systems to ensure compliance with our IT and Security policies.
- To ensure network and information security, including preventing unauthorised access to our computer and electronic communications systems and preventing malicious software distribution.
- To conduct data analytics studies to review and better understand Staff retention and attrition rates.
- Equal opportunities monitoring.

---

<sup>1</sup> The Trustees of Leonardo Electronics Pension Scheme, Leonardo Helicopters Pension Scheme and Leonardo FuturePlanner deem themselves to be data controllers when processing pension scheme member data; as such they are joint controllers of some of your information. The Trustees have put in place policies and processes to ensure compliance with data protection legislation. To view the Schemes' fair processing notices, please visit the publications section of the relevant scheme website ([leonardoelectronicspensions.co.uk](http://leonardoelectronicspensions.co.uk), [lhpensions.co.uk](http://lhpensions.co.uk), [futureplanner.co.uk](http://futureplanner.co.uk))



- In support of bid activities e.g. submitting work CV's as part of bid documentation.
- To assist with certain customers in identifying relevant employees for security purposes.
- Making visa applications for working overseas.

Some of the above grounds for processing will overlap and there may be several grounds that 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 or offer the contract we have entered/would enter into with you (such as paying you or providing a benefit), or we may be prevented from complying with our legal obligations (such as 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 reason and that reason is compatible with the original purpose. If we need to use your personal information for an unrelated purpose, we will notify you and we will explain the legal basis that allows us to do so.

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

## **7. How we use particularly sensitive information**

"Special Categories" of particularly sensitive personal information require higher levels of protection. We need to have further justification for collecting, storing and using this type of personal information. We have in place an appropriate policy document and safeguards that we are required by law to maintain when processing such data. We may process special categories of personal information in the following circumstances:

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

More rarely, we may process this type of information where it is needed in relation to legal claims or where it is needed to protect your interests (or someone else's interests) and you are not capable of giving your consent (such as if you are taken ill overseas on business), or where you have already made the information public. We may also process such information about Staff in the course of legitimate business activities with the appropriate safeguards.

#### *Our obligations as an employer*

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

- We will use information relating to leaves of absence, which may include sickness absence or family related leaves, to comply with employment and other laws.
- We will use information about your physical or mental health, or disability status, to ensure your health and safety in the workplace and to assess your fitness to work, to provide appropriate workplace adjustments, to monitor and manage sickness absence and to administer benefits.



- We will use information about your race, nationality or ethnic origin to ensure meaningful equal opportunity monitoring and reporting.
- We will use trade union membership information to pay trade union premiums, register the status of a protected employee and to comply with employment law obligations.

*Do we need your consent?*

We do not need your consent if we use Special Categories of your personal information in accordance with our written policy to carry out our legal obligations or exercise specific rights in the field of employment law. In limited circumstances, we may approach you for your written consent to allow us to process certain particularly sensitive data. If we do so, we will provide you with full details of the information that we would like and the reason we need it, so that you can carefully consider whether you wish to consent. You should be aware that it is not a condition of your contract with us that you agree to any request for consent from us.

## **8. Information about criminal convictions**

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 obligations at law (e.g. security vetting) and provided we do so in line with our data protection policy or security policies.

More rarely, we may use information relating to criminal convictions where it is necessary in relation to legal claims, where it is required to protect your interests (or someone else's interests) and you are not capable of giving your consent, or where you have already made the information public.

We do not envisage that we will hold information about criminal convictions as a matter of course but may need to do so from time to time in order to comply with security obligations.

We will only collect information about criminal convictions if it is appropriate given the nature of the role and where we are legally able to do so. Where appropriate, we will collect information about criminal convictions as part of the recruitment process or we may be notified of such information directly by you in the course of you working for us. Verification of any convictions held by an individual, which are considered "unspent" under the Rehabilitation of Offenders Act 1974, will be retained for the purpose of completion of Baseline Personnel Security Standards ("BPSS") Security Clearance

We are allowed to use your personal information in this way to carry out our obligations under the Official Secrets Act 1989 we have in place an appropriate policy and safeguards which we are required by law to maintain when processing such data, this includes technical and organisational safeguards such as encryption and only dedicated individuals having access.



## 9. Automated Decision-making

Automated decision-making takes place when an electronic system uses personal information to make a decision without human intervention. We are allowed to use automated decision-making in the following circumstances:

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

If we make an automated decision on the basis of any particularly sensitive personal information, we must have either your explicit written consent or it must be justified in the public interest, and we must also put in place appropriate measures to safeguard your rights.

You will not be subject to decisions that will have a significant impact on you based solely on automated decision-making, unless we have a lawful basis for doing so and we have notified you.

We do not envisage that any decisions will be taken about you using automated means, however we will notify you in writing if this position changes.

## 10. Data Sharing

We may have to share your data with third parties, including third-party service providers and other entities in the group. We require third parties to respect the security of your data and to treat it in accordance with the law. We may transfer your personal information outside the UK/EEA, such as to other companies within the Leonardo group or to third-party service providers. If we do, you can expect a similar degree of protection in respect of your personal data.

*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, such as the sale and purchase of goods and services relating to Leonardo's business or administering overseas contracts.

*Which third-party service providers process my personal information?*

"Third parties" includes third-party service providers (including contractors and designated agents) and other entities within our group. Those activities that may be carried out by third-party service providers typically include payroll, pension administration, benefits provision and administration, IT services, travel & expenses arrangements and company credit card.

This includes key suppliers:

- Accenture for Finance
- Aetna for International Health Care
- AIG for Reward
- AMEX for Expenses
- AON for Employee Benefits



- Avis for Car Rental
- AVIVA Care First for Employee Assistance Programme
- BSI Capita for Travel
- BUPA for Health Care
- Carlson Wagonlit Travel for travel
- Chubb Insurance and Helix International for employee travel insurance
- Concur for Travel & Expenses
- Coursera in the USA for training and development activities.
- DXC (Xchanging) for Contract Recruitment, Indirect Procurement and IT infrastructure
- EQA for Apprenticeship Management
- HIREVUE for Graduate/Apprentice recruitment
- Hyland (was Kofax) – for Employee files
- iJET for Travel Security Risk Management
- Insight Skills for Apprenticeship Management
- Iron Mountain for storage of documentation
- NGA HR for Apprenticeships, Payroll, Employment Contracts / Files, Travel, Recruitment & Reward
- Outposts for Apprenticeship Management
- Personal Group for Voluntary Benefits
- Tribal For Apprenticeship Management
- Unite for Trade Union
- Warwick – 1 for Apprenticeship Management
- XPS Administration for Pensions Administration
- Zellis for recruitment management activities

The Company also shares data with its parent company Leonardo SpA as part of Security and HR activities, as well as shared IT functions such as email servers.

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

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

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

We will share your personal information with other entities in our group as part of our regular reporting activities on company performance, in the context of a business reorganisation or group restructuring exercise, for system maintenance support and hosting of data and otherwise only for those purposes that are consistent with the purposes otherwise described in this policy.





### *What about other third parties?*

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

### *Transferring information outside the UK/EEA*

We will transfer the personal information we collect about you to the following countries outside the UK/EEA: the United States and India in order to perform our contract with you. There is not an adequacy decision by the European Commission in respect of either of those countries. This means that the countries to which we transfer your data are not deemed to provide an adequate level of protection for your personal information.

However, to ensure that your personal information does receive a proper and enforceable level of protection we have put in place Standard Contractual Clauses to ensure that your personal information is treated by those third parties in a way that is consistent with the EEA and UK laws on data protection.

Where your personal data needs to be exported in support of bid and/or commercial activity with an overseas customer/supplier this will be done in consultation with you to ensure that only the minimal amount of personal information necessary for the purpose is disclosed and that as far as possible your rights are protected. A typical example of this activity may be a sanitised work CV containing your experience and qualifications. The basis for such transfer in such cases is Compelling Legitimate Interest.

## **11. Data Security**

We have put in place appropriate technical and organisational measures to protect the security of your information. Details of these measures are available to employees on request from [Leonardo.SAR@leonardocompany.com](mailto:Leonardo.SAR@leonardocompany.com).

Third parties will only process your personal information on our instructions and where they have agreed to treat the information confidentially and to keep it secure.

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

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



## 12. Data Retention

### How long will we use your information for?

We will only retain your personal information for as long as necessary to fulfil the purposes we collected it for, including for the purposes of satisfying any legal, accounting, or reporting requirements. Details of retention periods for different aspects of your personal information are available in our retention policy which is available on the Company's intranet. To determine the appropriate retention period for personal data, we consider the amount, nature, and sensitivity of the personal data, the potential risk of harm from unauthorised use or disclosure of your personal data, the purposes for which we process your personal data and whether we can achieve those purposes through other means, and the applicable legal requirements.

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

In the case of job applicants that have been unsuccessful, we will only hold the personal data that you have provided as part of the application process for a maximum period of 12 months after which it will be permanently deleted. This specific retention period is in the event that the company wishes to make you aware of other job opportunities for which you may be suitable.

A copy of the Company's Data Retention Policy is available on request from [Leonardo.SAR@leonardocompany.com](mailto:Leonardo.SAR@leonardocompany.com).

## 13. 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 if your personal information changes during your working relationship with us e.g. change of address or marital status.

### Your rights in connection with personal information

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

- **Request access** to your personal information (commonly known as a "data subject access request"). This enables you to receive a copy of the personal information we hold about you and to check that we are lawfully processing it.
- **Request correction** of the personal information that we hold about you. This enables you to have any incomplete or inaccurate information we hold about you corrected.
- **Request erasure** of your personal information. This enables you to ask us to delete or remove personal information where there is no good reason for us continuing to process it. You also have the right to ask us to delete or remove your personal information where you have exercised your right to object to processing (see below).
- **Object to processing** of your personal information where we are relying on a legitimate interest (or those of a third party) and there is something about your particular situation which makes you want to object to processing on this ground. You also have the right to object where we are processing your personal information for direct marketing purposes.
- **Request the restriction of processing** of your personal information. This enables you to ask us to suspend the processing of personal information about you, for example if you



want us to establish its accuracy or the reason for processing it.

- **Request the transfer** of your personal information to another party.
- **To be informed** if we permit or become aware that a third party has shared your data in a way which does not conform the purposes outlined in this document.

If you want to review, verify, correct or request erasure of your personal information, object to the processing of your personal data, or request that we transfer a copy of your personal information to another party, please contact the Company's Data Protection Management Team via [Leonardo.SAR@leonardocompany.com](mailto:Leonardo.SAR@leonardocompany.com).

### **No fee usually required**

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

### **What we may need from you**

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

## **14. RIGHT TO WITHDRAW CONSENT**

In the limited circumstances where you may have provided your consent to the collection, processing and transfer of your personal information for a specific purpose, you have the right to withdraw your consent for that specific processing at any time. To withdraw your consent, please contact the Company's Data Protection Management Team via [Leonardo.SAR@leonardocompany.com](mailto:Leonardo.SAR@leonardocompany.com) or your HR representative. Once we have received notification that you have withdrawn your consent, we will no longer process your information for the purpose or purposes you originally agreed to, unless we have another legitimate basis for doing so in law.

## **15. USE OF EMPLOYEES/CONTRACTORS IN DEVELOPING AND TESTING PRODUCTS AND SERVICES.**

Leonardo has a legitimate interest in supporting the testing, development and demonstration of Leonardo products and services. In order to achieve this we may occasionally need to include some personal data of employees/contractors to support these activities. For example, if we are developing a camera to feed a facial recognition system we need to capture images of real people to test that. All such activity is subject to careful consideration of data protection matters and each project will develop appropriate analysis of risk balance, control measures and communications to affected employees/contractors to ensure the rights of individuals are respected in accordance with company protocols. No such tests etc. will be conducted without the impacted individuals being made aware beforehand and being given the opportunity to object. The general information in this notice will be supplemented by project specific data privacy notices communicated to relevant employees/contractors where necessary.

- *The kind of information we hold about you* – images, voice recordings, technical information about you such as an IP address, registration mark of a vehicle or serial number of an asset associated with you. It is very unlikely that any special category

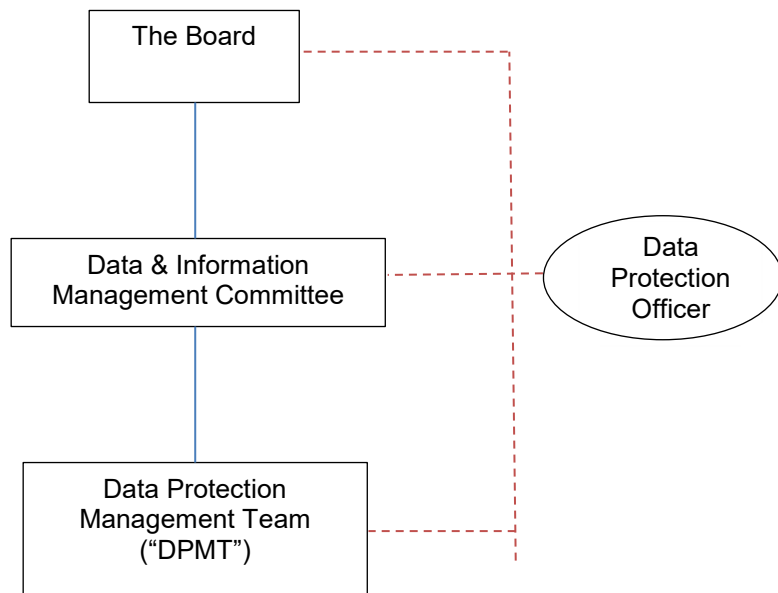


information would be captured, if it were a specific arrangement would be put in place and communicated to you.

- *How is information collected?* – using systems made, engineered or under test by Leonardo as part of its business providing products and solutions to customers.
- *How will we use the information about you?* – to enable testing, development and demonstration of Leonardo products and customer solutions to show that where interactions with natural living persons are an inherent part of the operation of the product or customer solution that these operate correctly. This is typically because of the company’s legitimate interest in developing new products, or to satisfy the needs of a contract. In some circumstances we may need to use this information to protect your or someone else’s interests – in particular the safety of people involved in the activity. It should be noted that, whilst the information collected about you is of course real, it is being used in a simulated environment thus the risk of adverse impact to your rights through incorrect processing are very low (for example if we were testing an artificial credit scoring system using your data, this would not affect your real world credit score).
- *Situations in which we will use your information* – in conducting testing, development and demonstration of Leonardo capabilities. We will only use real data where it is impractical to use simulated/synthetic or pseudonymised/anonymised data.
- *How will we use particularly sensitive information?* – only in specific circumstances with suitable arrangements in place and communicated to affected individuals in advance.

## 16. Data Protection Management

We have established a Data Protection Management Structure within the Company:



The Terms of Reference for the DPMT are attached in the Annex



## 17. Processing of Under18's Personal Data

The Company will occasionally process the personal data of children, i.e. those younger than 18 years of age. Examples of such occasions include:

- Bring child to work day;
- STEM activities/school engagements;
- Work experience; or
- Apprenticeships (under 18).

Each such activity constitutes a Legitimate Interest of the Company. In light of the particular requirements associated with the Processing the Personal Data of Children, the Company will engage directly with either the relevant school or parent/guardian to ensure that any such Processing is understood and correct.

Under certain exceptional circumstances, the Company is required by law to make disclosures to regulatory bodies or social services. Any such disclosure will always be done in full compliance with the relevant laws and guidance such as Keeping Children Safe in Education.

## 18. Changes to this Privacy Notice

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

**If you have any questions about this privacy notice, please contact** the Company's Data Protection Management Team or the Data Protection Officer via [Leonardo.SAR@leonardocompany.com](mailto:Leonardo.SAR@leonardocompany.com)

Or you can contact the Information Commissioners Office on: [casework@ico.org.uk](mailto:casework@ico.org.uk) citing our Registration Number Z6375415.

Signed for and on behalf of Leonardo UK Ltd:

.....

**James Wells**  
**Data Protection Officer**



## **Annex**

### **Data Protection Management Team Terms of Reference**

## Terms of Reference for the Data Protection Management Team

### 1) Purpose and Authority

The Data Protection Management Team is a Sub-Committee of Data and Information Management Committee (“the Committee”), duly convened to support the Committee on Data Protection: being the prevention of an adverse impact on the rights of Data Subjects (as defined by Data Protection Act 2018 and the General Data Protection Regulation(EU) 2016/679 (“GDPR”)) with whom the Company interacts with or has an impact on; and to minimise the risk to the Company of regulatory intervention or sanction by implementing robust policies and procedures for the management of Personal Data.

Core responsibilities shall be:

- Oversight and mitigation of the Company’s GDPR risk profile;
- Supporting Divisions in the discharge of their GDPR responsibilities by acting as Subject Matter Experts;
- Managing Data Subject Access Requests;
- Managing the Data Processing Register;
- Managing any Data Protection Breach in accordance with the Protocol;
- Overseeing the implementation of the Company’s Data Protection Policy Portfolio and ensuring the Company’s policies and procedures are fit for purpose and up to date;
- Support engagement with external stakeholders in respect of GDPR matters arising as directed by the DPO;
- Supporting any transparency matters (journalists, declarations etc.);
- Promoting effective working practices with regard GDPR activity;
- Establishing metrics to determine the effectiveness of the Company’s GDPR compliance strategy, such as:
  - Number of Data Subject Access Requests in a quarterly period
  - Number of reported breaches in a quarterly period
  - Number of privacy impact assessments undertaken in a quarterly period
  - Changes of risk assessment status in the quarterly period.
- Conduct an annual review or as necessary of the Company’s GDPR compliance strategy including making recommendations to Divisions/ Functions/ Data Management Committee body;
- Be responsible for continuous improvement of the GDPR process; and
- Delegation and management of activities to the Satellite Teams.

The Sub-Committee has been established under the authority and at the absolute discretion of the Committee, which shall retain the power to disband it. The Sub-Committee’s scope and authority to act shall be set by these Terms of Reference, which have been approved by the Committee.

The Sub-Committee shall remain accountable to the Committee for their work.

## **2) Membership and term**

The Sub-Committee shall include a Chairman and representatives from the following areas:

- human resources;
- IT;
- security;
- legal;
- risk management; and
- shall ensure that there are influential representatives from each of the Divisions.

Others may be invited by the Chairman (or in their absence, his or her deputy) to attend all or part of any meeting.

Appointments may be made as deemed necessary to ensure the effectiveness of the Sub-Committee, subject to a right of veto by the Committee. Each Sub-Committee member must resign upon ceasing their employment with the Company or at the request of the Chairman.

Membership and composition shall be considered at least annually. There shall be no fixed term of office.

Membership may not be less than six (6).

## **3) Chairman**

The Chairman of the Committee shall be the Company's Data Protection Officer or their nominee. In the Chairman's absence, his nominated deputy shall act as Chairman.

The Chairman shall lead the Sub-Committee and demonstrate objective judgement throughout their tenure, promoting a culture of openness and debate. The Chairman shall facilitate constructive Sub-Committee relations and the effective contribution of all Members. The Chairman, supported by the secretary, shall also ensure that the Sub-Committee receive accurate, timely and clear information.

## **4) Secretary**

The statutory Company Secretary of the Company or their nominee shall act as the Secretary to the Sub-Committee.

## **5) Quorum**

The quorum necessary for the transaction of business shall be 3 members of whom at least one must be either the Chairman or their nominated deputy.

A duly convened meeting of the Sub-Committee at which a quorum is present shall be competent to exercise all or any of the authorities, powers and discretions vested in, or exercisable, by the Sub-Committee.

## **6) Frequency of meetings**

The Sub-Committee shall meet quarterly.



### **7) Notice of meetings**

Meetings of the Sub-Committee, other than those regularly scheduled as above, shall be summoned by the Secretary at the request of the Chairman.

Unless otherwise agreed, notice of each meeting confirming the venue, time and date together with an agenda of items to be discussed and supporting papers, shall be forwarded to each member of the Sub-Committee and any other person required to attend, no later than five (5) working days before the date of the meeting.

### **8) Conduct of meetings**

Except as outlined in these Terms of Reference, meetings of the Sub-Committee shall be conducted in accordance with the provisions of the Company's Articles of Association, governing the proceedings of directors;

In accordance with the Company's Articles of Association, a decision of the Sub-Committee shall be taken where the members indicate to one another (by any means) that they share a common view on a matter, exercising their collective responsibility and it is recorded in writing.

A decision may not be taken if the eligible Sub-Committee members would not have formed a quorum at such a meeting.

### **9) Minutes of meetings**

The Secretary shall record the attendance, proceedings and decisions taken at all meetings of the Sub-Committee. The Secretary shall also record all invited persons who are present for all or part of the meeting.

Minutes of meetings shall be circulated promptly to all members of the Sub-Committee.

### **10) Reporting responsibilities**

The Chairman shall report formally to the Committee Chairman on the proceedings of all Sub-Committee meetings in a timely manner.

### **11) Annual effectiveness review**

The Sub-Committee shall arrange for periodic reviews of its own membership, performance and these Terms of Reference annually, to ensure that the Sub-Committee is operating effectively. Changes to these Terms of Reference must be approved by the Committee.