Amphenol Employee Data Protection Notice
UK, EEA and Switzerland (Issue 3 – September 2025)

Amphenol needs to process and retain certain information regarding its employees' personal data. Amphenol is respectful of such information and is committed to protecting it in line with applicable data protection laws, including the EU General Data Protection Regulation and its UK equivalent ("GDPR").

Data protection legislation regulates the way in which certain data about you, both in paper and electronic form, is held, used, transferred and disclosed. This Notice will give you some useful information regarding the type of data that Amphenol and its affiliates in the United Kingdom ("UK"), the European Economic Area ("EEA") and Switzerland (the "Company") may keep about you and the purposes for which it is kept.

This Employee Data Protection Notice relates and applies to the personal data of employees (both current and former) that are Processed by the Company. "Processing" includes the collection, storage, retrieval, alteration, disclosure or destruction of personal data.

For further information on the principles applied by the Company to protect its employees' personal data, please refer to the Amphenol Employee Data Protection Policy, available from the HR Department.

1. How the Company Uses Your Personal Data

Throughout employment and for as long as is necessary after the termination of employment, the Company may Process your personal data for purposes connected with your employment, including, but not limited to: recruitment, appraisals, performance, promotion, training, discipline, grievances, complaints, and termination of your employment, administration, reporting, management and resource planning (together "HR management"), employee directory, pay and remuneration, benefit entitlements, such as pension and insurance and other benefits, tax, other deductions from pay, health and safety, security checks and clearance, IT operation and maintenance: (i) to ensure compliance with legal and regulatory requirements, (ii) to comply with our contractual obligations under an employment agreement with you, or (iii) where this is necessary for legitimate interests pursued by the Company or a third party and your interests and fundamental rights do not override those interests. The Company may Process your personal data for security and safety reasons, including for monitoring and controlling access to the Company's premises, and for access badge management purposes, in order to ensure compliance with legal and regulatory requirements or where this is necessary for legitimate interests pursued by the Company or a third party.

If you raise a grievance, make a complaint, or blow the whistle, we will process your personal data, and any personal data that has been provided about you as part of the grievance, complaint or whistleblowing disclosure, in order to investigate the grievance, complaint or disclosure. We are either under a legal obligation to process your personal data in this way

(e.g., under the Whistleblowing Directive or local employment legislation that requires us to ensure we operate a fair process in disciplinary proceedings) or it is in our legitimate interests to process your data for these purposes because we want to protect our staff, property, assets and/or reputation.

The Company may also Process personal data, including special categories of personal data as described below, if it is necessary to do so for compliance with any legislative requirement. Please see the details of the lawful grounds for processing personal data Amphenol relies on under the GDPR in the table in section 2 below.

2. The Personal Data Collected by the Company

The types of personal data that the Company may Process includes, but is not limited to, your:

- Personal details – Employee name, home address, e-mail address, telephone number (including personal mobile number) and other contact information, national identity/registry/insurance/social security numbers, images, date of birth, citizenship and nationality, gender, details of language skills, and where applicable by law, details regarding military service;
- Family & social – Family composition (including marital status or partnership, names of spouse and/or dependants and/or next of kin and relationship), nominated beneficiaries and emergency contact details;
- Education and training - Educational and vocational training (including qualifications, grades, attendance at educational establishments and training received) student status and spoken/written/reading language proficiency;
- Employment details – Status of employment, performance ratings, work time/utilisation records and forecasts, training records, evaluations, holiday or annual leave arrangements, terms of labour contract, details of any disciplinary actions, health and safety data, employee benefit plan participation details, work authorisation/eligibility/permit/visa requirements/status, stock option grants, grant number and type and value, employee number, company ID number, business title/unit/department/location, job functions and description, working arrangements (full/part-time), job location(s), seniority data, retirement age, contract length, hire/re-hire/termination date and codes, supervisor hierarchy, line management details, security clearance, work history and experience, business travel arrangements, details of mobility/willingness to relocate, workplace accident information, occupational health information, information about a grievance, complaint or whistleblowing disclosure by or involving you;
- Salary information – Salary information, expense reimbursement, benefit information, bank account details, direct deposit/credit arrangements, pension payment and stock option information (stock grants or option exercise details), bonus, additional pay, variable compensation awards, tax data (national and local), flexible spending enrolments, grant valuation information, paid time off and credit card details (personal and business).

Purpose of processing	Categories of personal data	Lawful basis under the GDPR
Human resources management	Personal details, employment details, education and training	Legitimate interests to manage human resources or a legal obligation (e.g. whistleblowing procedures or health-related data)
Employee directory	Education and training, employment details	Legitimate interests to administer an employee directory
Pay and remuneration	Salary information	Performance of contract
Benefit entitlements (includes benefits for next of kin, dependents, beneficiaries)	Family & social	Performance of contract or a legal obligation
Organisational analysis, development and management	Salary information	Legitimate interests to ensure business efficiency
IT and security implementation, operation and maintenance	Information about a device used, personal details. Customer and supplier contact details	Legitimate interests to protect staff, property, and assets
Legal compliance, advice and defence	Any information above	Legal obligation or legitimate interests to exercise or defend legal claims

3. The Special Categories of Personal Data Collected by the Company

Where required by local laws, and in some very exceptional cases, the Company may hold special categories of personal data (also known as sensitive data) about you. This type of data may include information about your health, racial or ethnic origin, political opinions, religious or philosophical beliefs, or criminal records. Where collected, these special categories of personal data will be Processed to meet the Company's legal responsibilities or, where necessary, for personnel management and administration, for example, suitability and fitness for employment, insurance, sick pay and sick leave, absences, maternity and parental leave and entitlement and safe working environment.

The Company may, in certain circumstances, ask you for your explicit consent to any Processing, unless the Company Processes such special categories of personal data because it is legally required to do so or where otherwise permitted by law. Where the Company is legally required to obtain explicit consent, it shall only Process special categories of personal data subject to your freely given and unambiguous consent.

4. How the Company Protects Personal Data

The Company will take all steps reasonably necessary to ensure that there are appropriate security measures in place to safeguard your personal data. In determining the appropriate security, the Company takes into account technological developments and assesses the measures in place against the risk of harm that may result from a security breach. The security measures implemented by the Company are appropriate to protect against the risks presented by the Processing and are put in place to prevent unauthorised disclosure, loss, destruction or damage to your personal data.

5. With Whom the Company Shares Personal Data

Your personal data may be shared across the Company and its affiliates, where necessary, to fulfil legitimate business purposes or to comply with applicable legal requirements.

The Company may also share your personal data with certain third parties and service providers (e.g. insurers, legal and other professional advisers, company credit card providers, pension scheme administrators, providers in charge of performing security checks, operators of our whistleblowing hotline that it has retained to perform services on its behalf, to provide employment/related benefits, or for legal/regulatory purposes. The Company prohibits these third parties from using or disclosing your personal data except as necessary to perform services or to comply with legal requirements. The Company may disclose your personal data without offering you an opportunity to opt out of such disclosure: (1) as permitted by law or required by legal process; (2) to law enforcement authorities or other government officials; or (3) when the Company believes disclosure is necessary or appropriate to prevent physical harm or financial loss or in connection with an investigation of suspected or actual illegal activity.

The Company reserves the right to transfer any personal data it has about you in the event that the Company sells or transfers all or a portion of its business or assets, without offering you the opportunity to opt out of such transfer (except where required by local law). Should such a sale or transfer occur, the Company will use reasonable efforts to direct the transferee to use employee personal data in a manner that is consistent with this Employee Data Protection Notice.

6. International Transfers of Personal Data

The personal data the Company holds will be for management and administrative use only but the Company may, from time to time and subject to the appropriate safeguards, need to transfer personal data it holds about you to relevant third parties internationally, for example,

for the purposes of recruitment, secondment or other purposes arising out of a Company policy.

The personal data that the Company collects from you may be transferred to, and stored at, a destination outside the UK, the EEA and Switzerland. It may also be Processed by the Company staff operating outside the UK, the EEA and Switzerland, or one of its affiliates, or data processor(s) engaged by the Company. Some of these destinations do not offer the same statutory protection for personal data as exists within the UK, the EEA and Switzerland. Such transfers will be for the same limited purposes, and under similar security conditions, as those applicable to the Processing of your personal data in your country. The transfers are made subject to a personal data export agreement pursuant to which members of the Company outside the UK, the EEA and Switzerland or data processors outside the UK, the EEA and Switzerland accept a personal data protection regime which is the same in all material aspects as the UK/EU/Swiss regime.

7. Your Rights Under Applicable Laws

You may have the right to request access to, correction or erasure of, or to object to, personal data processed by the Company about you. You can find more information about these rights, and how to exercise them, in the Amphenol Employee Data Protection Policy.

8. Questions or Concerns About Your Personal Data

If you have any concerns regarding the Processing of your personal data as described throughout, please contact your Human Resources Manager. The Company will take appropriate steps to address any inquiries or complaints. The Company also cooperates with relevant data protection authorities for complaints concerning its handling of your personal data.