PRIVACY NOTICE (STAFF)

Updated: 12 June 2019

Background

Curtiss-Wright Corporation (CW) is a diversified, multinational provider of highly engineered, technologically advanced products and services and to manage our business and meet contractual obligations we need to collect and process personal data relating to our employees to manage the employment relationship.

CW is committed to meeting its data protection obligations and being transparent about how it collects and uses employee personal data. For the purposes of this privacy notice, 'employee' means job applicants, employees, workers, contractors, volunteers, interns, apprentices and former employees.

Purpose

This privacy notice describes how CW, as Data Controller, collects, uses and protects your personal data and your associated individual rights and obligations. This privacy notice does not apply to the personal data of anyone not categorised as an employee.

This privacy notice supports CW (Privacy) Policy No. 30 [https://insidecw.com/resources].

Why We Process Your Personal Data

CW processes personal data relating to those we employ to work at CW under the lawful basis of **CONTRACT**, i.e. fulfilling the contract of employment. We need to process your data to pay you in accordance with your employment contract and to administer benefit, pension and insurance entitlements. We need to process data to manage careers (including appraisals, promotion and succession planning and talent management), training and development, disciplinary, grievance and termination processes, communicating with employees and/or their representatives, monitoring and managing travel arrangements.

In some cases, CW needs to process personal data under the lawful basis of **LEGAL OBLIGATION**. For example, CW is required to check an employee's entitlement to work in the country of employment, to deduct tax, to comply with health and safety laws and to enable employees to take periods of leave to which they are entitled. For certain positions, it is necessary to carry out criminal records checks and restricted party screening checks to ensure that individuals are legally permitted to undertake the role in question.

CW also needs to process personal data under the lawful basis of **LEGITIMATE INTEREST** in that we have a legitimate interest to process your personal data throughout all stages of the employment relationship. Processing employee data in this way will allow us to:

- Support CW's legitimate business aims and deliver operational processes and tools that schedule work and manage company assets;
- Support the CW Human Resource functional area in regard to recruitment and promotion; employee and emergency contact details; contractual and statutory rights; health and wellbeing initiatives; disciplinary and grievance; codes of conduct; employee performance; career development; succession planning and absence management; holiday entitlements; salary, pensions, insurances, assurances and benefits entitlements;
- Support the CW Information Technology (IT) functional area in regard to internal networks and other IT systems in line with CW IT policies and guidelines;
- Support CW Security programmes that maintain physical security of and control access to CW facilities, offices, equipment and information;
- Support CW obligations to employee health and safety at work; in obtaining occupational health advice; by ensuring CW complies with obligations to individuals with disabilities; to meet our obligations to national health and safety law;
- Support CW legitimate business aims; to support legal counsel and contract teams; to exercise or defend legal proceedings; to obtain legal advice to protect CW against damage, injury, theft, legal liability, fraud,

abuse or other misconduct; to comply with legal or regulatory compliance obligations; to maintain and promote equality in the workplace.

What Personal Data Is Processed

CW collects and processes a range of personal data about you. This includes:

- Your name, address and contact details, including email address and telephone number, date of birth and gender;
- The terms and conditions of your employment;
- Details of your qualifications, skills, experience and employment history, including start and end dates, with previous employers and with Curtiss-Wright;
- Information about your remuneration, including entitlement to benefits such as pensions or insurance cover;
- Details of your bank accounts, in certain circumstances we may provide salary and appointment confirmation references for mortgage and other financial applications;
- Information about your marital status, spouse or partners, dependants, beneficiary information and emergency contacts. This may include divorce or legal separation details and official name changes;
- Information about your nationality including national identification numbers, place and country of birth and entitlement to work in the country of employment;
- Personally identifiable images. In certain locations we may operate CCTV surveillance cameras;
- Information about any criminal record you may have (subject to rehabilitation of offenders legislation);
- Details of your schedule (days of work and working hours) and attendance at work;
- Details of periods of leave taken by you, including the reasons for the leave, whether for holiday, sickness absence, maternity, paternity and other family leave requirements or sabbaticals;
- Details of any disciplinary or grievance procedures in which you have been involved, including any warnings issued to you and related correspondence;
- Assessments of your performance, including appraisals, performance reviews and ratings;
- Training you have participated in, performance improvement plans and related correspondence.

We process the personal information of your emergency contacts under legitimate interest as it is necessary for us as a good employer to contact someone if you are taken ill or injured at work. We only collect the minimum amount of data and we will only use it in an emergency. You have the right not to provide us with emergency contacts data.

Special Category Data

To the extent that we need to collect, hold or otherwise process any special categories of data about you, we will ensure that you are informed of such processing. Where required by law, we will obtain your explicit consent to the processing and particularly to the transfer of such data to any non-CW entities. Appropriate security measures (e.g., physical security devices, encryption, and access restrictions) will be taken depending on the nature of these categories of data and the risks associated with the intended uses.

Some special categories of personal data, such as information about health or medical conditions, are processed to meet our employment law obligations (such as those in relation to employees with disabilities and for health and safety purposes). If applicable, information about trade union membership may be processed to allow CW to operate check-off for union subscriptions. Where CW processes other special categories of personal data, such as information about ethnic origin, sexual orientation, religion or belief, this is done for the purposes of equal opportunities monitoring.

How We Collect Your Personal Data

CW collects personal data in a variety of ways. For example, data is collected through application forms, CVs or resumes, your passport or other government issued identity documents, your driving licence or forms completed

by you at the start of or during employment (such as benefit nomination forms), from correspondence with you, verbally through interviews, meetings or other assessments.

In certain locations, CW will process your personally identifiable images via CCTV surveillance systems for reasons that may include the prevention and detection of crime, safeguarding staff and visitors, ensuring compliance with health and safety procedures and improving productivity.

In some cases, CW collects personal data about you from third parties, such as references supplied by former employers, personal contacts or information from employment background check providers. In certain circumstances, CW may receive information from credit reference agencies, criminal records checks permitted by law or information from disclosed barring service and restricted party screening agencies. We may collect sensitive medical or other special category information provided by you during health surveillance screening or other legally mandated activities required of an employer.

Principles for Processing Personal Data

As the data controller, CW is accountable to you and to the supervisory authorities for how we process your personal data. CW will observe and be able to demonstrate compliance with, the key principles of processing. Personal data will be:

- Processed lawfully, fairly and in a transparent manner;
- Collected for specified, explicit and legitimate purposes and not processed further in ways incompatible with those purposes;
- Adequate, relevant to and limited to what is necessary. For example, we will not hold more information than is required for the specific purpose;
- Accurate and where necessary, kept up-to-date. Every reasonable step will be taken to ensure the personal data we hold is not incorrect or misleading as to any matter of fact;
- Not kept for longer than we need it. CW Record Retention Policy No. 5 has standard data retention periods that wherever possible, comply with documentation requirements;
- Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage;
- Processed in consideration of the requirements of accountability and the above mentioned principles of data processing, using appropriate technical or organisational measures.

Sharing Your Personal Data

Your personal data will be shared with other CW employees within HR and recruitment departments, finance and payroll teams, your line manager, other managers in the business area in which you work and IT staff if access to the data is necessary for performance of their roles.

CW also shares your personal data with contracted third parties that process your personal data on our behalf in connection with payroll and pension providers, state and local government agencies (e.g. tax, pension, social security and social benefits), occupational health services providers, shared service providers (e.g. travel expenses, human resource interfaces), business management systems (e.g. environment, customer or supply chain etc.).

In some cases, CW will share your personal data with third parties to fulfil legal obligations, such as providing information to government authorities or any other legally mandated activity required of an employer.

Your personal data may be transferred to and stored in a country whose laws do not provide equivalent protection to that which applies in your home country. In such circumstances, we will implement contractual or other measures to ensure an adequate level of protection for your personal information. All our affiliates and third-party agencies will be required to comply with this privacy notice or to guarantee equivalent levels of protection when processing your personal information.

Protecting Your Personal Data

CW takes the security of your personal data seriously and has internal policies and controls in place to try to ensure that your data is not lost, accidentally destroyed, misused or disclosed and is not accessed except by its employees in the performance of their duties.

Where CW engages third parties to process personal data on its behalf, they do so on the basis of contractually binding instructions. They are also under a duty of confidentiality and are obliged to implement appropriate technical and organisational measures to ensure the security of your personal data.

Storing Your Information

Your personal information will be stored on secure servers or systems owned or operated by Curtiss-Wright both within and outside the European Economic Area (EEA).

Within CW your information will be stored in accordance with the CW Information Security Policy. Where your information is stored in countries outside the EEA or a country approved by the EU we will ensure it is protected by encryption during transmission.

Personal data gathered during the employment is held in the individual personnel file (in hard copy or electronic format, or both) and on numerous shared service and business management systems and other IT systems, including MS Outlook.

Record Retention

CW will retain your personal data in accordance with legal and regulatory requirements. [CW Policy No5 Record Retention and Schedules] refers and can be found on InsideCW in Legal Policies.

Your Individual Rights

Where our processing of your personal data is governed by EU/UK data protection laws, you have certain rights in relation to your personal data. You have the right to:

- Be informed about the collection and use of your personal data. You have received this information within this privacy notice;
- Access your personal data;
- Have inaccurate personal data rectified, or completed if it is incomplete;
- Have personal data deleted or destroyed in certain circumstances, for example if (i) it is no longer necessary for us to process your personal information for the purposes for which it was originally collected or (ii) you withdraw your consent to our processing, where consent is the only legal basis on which we rely to process your personal information or (iii) your personal information has been unlawfully processed or (iv) it is necessary for us to erase your personal information for compliance with applicable law;
- Request the restriction or suppression of the processing of your personal data;
- Data portability that allows you to obtain and reuse your personal data for your own purposes across different I.T. services;
- Object to processing that is likely to cause, or is causing you, damage or distress. You have an absolute right to stop your data being used for direct marketing purposes;
- Understand whether or not Curtiss-Wright is conducting automated decision-making or profiling and the logic involved in any such decision-making or profiling.

You should be aware that not all your data subjects' rights are absolute and will apply in certain circumstances only. For example, CW is obliged to maintain certain records for legal reasons and in this scenario, you would be unable to have data deleted or destroyed.

How you can access your information

To exercise your rights you will need to make a Data Subject Access Request (DSAR) verbally or in writing to the CW DPO (details below). CW will respond to a request without undue delay and at the latest within one month from the date it is received.

Once satisfied the request is genuine, a process that may include identity verification of the requestor, CW will provide the data subject with an electronic copy of the personal data requested.

CW reserves the right to extend the time to respond to a DSAR by a further two months if the DSAR is complex or the data subject has submitted a number of requests. In the event an extension is deemed necessary, CW will inform the data subject within one month of receiving the DSAR and explain why the extension is necessary.

If a DSAR is manifestly unfounded or excessive, CW is not obliged to comply with it. Alternatively, CW can agree to respond but will charge a fee, which will be based on the administrative cost of responding to the request. A DSAR is likely to be manifestly unfounded or excessive where it repeats a request to which we have already responded. If an individual submits a request that is unfounded or excessive, CW will notify the data subject that this is the case and whether or not it will be responded to.

If you have concerns with how we are using your information or how we have responded to your request, you may register such concern with the DPO or you can contact the CW legal department. Alternatively, you have the right to complain to the supervisory authority that protects the personal data in the country where you are resident.

Obligations to Supervisory Authorities

CW will respond diligently and appropriately to requests from supervisory authorities about this privacy notice or any query or investigation concerning our compliance with applicable data protection laws. Should you receive any such requests, you should contact the CW DPO immediately using the contact details at the end of this privacy notice.

Individual Employee Responsibilities

Employees are responsible for helping CW keep their personal data up to date and should let CW know if any data previously provided to CW changes, for example if an individual moves house or changes bank details.

Employees may have access to the personal data of other employees in the course of their employment. Where this is the case, CW relies on these individuals to help meet its data protection obligations. Employees who have access to personal data are required:

- To access only data that they have authority to access and only for authorised purposes;
- To not disclose data except to individuals (whether inside or outside the organisation) who have appropriate authorisation;
- To keep data secure (for example by complying with rules on access to premises, computer access, password protection, secure file storage and destruction);
- To not remove personal data or devices containing personal data or devices that can be used to access personal data, from the CW premises without adopting appropriate security measures (such as encryption or password protection) to secure the data and the device;
- To not store personal data on local drives or on personal devices that are used for work purposes;
- To report data breaches of which they become aware to the CW DPO immediately.

Failing to observe these requirements may amount to an offence, which will be dealt with under the CW disciplinary procedures. Significant or deliberate breaches of this policy, such as accessing employee or customer data without authorisation or a legitimate reason to do so, may constitute gross misconduct and could lead to dismissal without notice.

Training

CW will provide training to all new starter EU/UK employees about their data protection responsibilities as part of the induction process. All EU/UK employees will receive regular data protection training.

Employees whose roles require regular access to personal data, or who are responsible for maintaining or implementing contracts with third party data processors, or are responsible for implementing the requirements of this privacy notice will receive additional training to help them understand their data protection responsibilities.

Privacy Notice Updates & Availability

This [CW Privacy Notice - Staff] is on both the Corporate SharePoint and the [InsideCW - Legal - GDPR] sites. We may need to update this privacy notice periodically so we recommend that you revisit this information from time to time. This version was last updated on the date stated in document footer.

Data Privacy Support

Should you need local and general data privacy guidance, you can contact your CW Human Resources Manager or you can visit the website of the supervisory authority that protects the personal data in the country where you are resident.

However, if you need specific data privacy advice or you have questions about this policy notice or any other aspect of data privacy, please contact the CW DPO:

- By Post
  Data Protection Officer
  Curtiss-Wright
  15 Enterprise Way, Aviation Park West, Bournemouth Airport, Christchurch, BH23 6HH, UK.

- By Email (helpdesk)
  CWDPHelpdesk@one.curtisswright.com

- By Telephone
  +44 (0) 1202 034000

Geoff Austin
Data Protection Officer