| Falck | Always check on-line for validity. **Privacy Commitment to Employees including Job Applicants** | | | | Level: **Support Processes** Approved by: **claire.ward 16.10.2018** |
|---|---|---|---|---|---|
| Document users: **FalckUK-AMB** | Editor: **claire.ward** | Responsible: **HeadHSEQ** | Document number: **45706** | Version: **1** | |



## 1) Introduction

1.1 As an employer, Falck UK Ambulance Service Limited (Falck UK) acts as data controller for certain personal data about employees including job applicants.

1.2 Falck, as a data controller, has a duty to protect the personal data we process about our employees. You can read more about the framework for processing personal data in our General Data Protection Regulation (GDPR) Policy and Falck Group's Personal Data Protection Policy and Information Security Policy. We have a suite of information governance, information technology (IT), and records management policies (information governance policies), which should be read in conjunction with this privacy commitment, and have accreditation for ISO 27001: Information Security.

1.3 This privacy commitment describes our processes for collecting, holding, using and transferring of the personal data of our employees. Together with or commitment to patients, this document sits within our framework of information governance policies and processes and is overseen by the Head of Health Safety Environment and Quality (HSEQ), with support from our IT services provider.

1.4 This commitment defines, to our employees, our responsibility for protecting their personal data in accordance with the European Union (EU) General Data Protection Regulation (GDPR), effective from May 2018. Consequently, it is worded in terms that express these responsibilities.

1.5 Personal information, held about you, our employees, will not be shared, sold or disclosed in any manner other than as described in this privacy commitment.

1.6 In accordance with our Governance Framework, our privacy commitment to employees and patients, and all other information governance policies will be reviewed and audited annually by the HSEQ Team to ensure fitness for purpose and compliance annually by the HSEQ Team.

## 2) Responsibilities

2.1 The Data Protection Officer (DPO) for Falck Group is: Birgitte Poulson, who may be contacted at: DPO@falck.com or +45 30 50 18 46.

2.2 Responsibility for GDPR compliance in the United Kingdom is delegated to the Director of Quality & Operations; who has responsibility for the administration and implementation of Falck UK's GDPR Policy.

2.3 These executive responsibilities are delegated to the Head of HSEQ. Therefore this commitment, which was prepared by Falck Group, was modified for Falck UK by the Head of HSEQ. Future reviews will also be conducted by the Head of HSEQ.

2.4 All directors and managers are responsible for ensuring that their teams are aware of their responsibilities in relation to the collection, storage and handling of the personal data of employees and of their obligation to provide personal data relevant to their employment. These responsibilities are outlined within our information governance, records management and IT policies.

2.5 All employees are responsible for complying with the requirements of this commitment to protect the personal data of their colleagues.

## 3) Procedures

3.1. Statement to employees

3.1.1 Your employee file can be found in Falck's electronic human resources system. Access to this file is limited to solely those employees whose role requires them to use the information retained. This is largely limited to the Recruitment and Human Resources Teams and your line manager.

3.1.2 You are required to provide personal information to enable Falck to enter into an employment relationship with you, and agree a contract with you. If you do not provide the necessary requested information you will not be able to work for Falck.

3.1.3 Further if any of our processing is dependent upon your consent you have a right to withhold or withdraw such consent, which means that the information can no longer be processed by Falck, unless the processing can be based on another legal basis. The withdrawal of the consent, will not affect the processing already incurred prior to that withdrawal.

3.1.4 However, you need to be mindful of you obligation, as an employee, or potential employee, to provide relevant personal data, relevant to your role, for your sustained employment, e.g. we require a Disclosure and Barring Service check, and our consequential ability to terminate your employment should you fail to provide necessary information.

3.1.5 You have, with the limitations of the legislation, among other things right to access your personal data, right to rectify incorrect information, right to deletion of information, right to limit information, right to data portability and right to object to the processing of personal data, including automated, individual decisions.

3.1.6 All employees are encouraged to raise concerns about the treatment of personal data and report incidents where their security may have been breached. You may do this by using our incident reporting or whistleblowing processes as outlined in the relevant policies.

3.1.7 You also have a right to raise a concern with the Information Commissioner's Office, as the supervisory authority [https://ico.org.uk/].

3.2. Collection of information

3.2.1 Personal data, which is held in accordance with our human resources policies and processes, held about you may include:

- Name, address, e-mail address and telephone number
- Identity information, including national insurance number
- Date of employment, place of employment and job title
- Working hours, including duty and duty hours
- Holiday and other absence
- Sick leave
- Salaries and pensions, wage subsidies, information relevant to payroll
- Bank details
- Tax information
- Salary deductions and salary sacrifices, including childcare vouchers and to ride to work
- Information related to occupational injuries and special employment
- Personnel administrative information, such as education and qualifications, courses, competence profile, job wishes, employee development talks, ratings, employment, trusts, loans of various effect
- References
- Contact information on your next of kin
- Disclosure and barring
- Personality test
- Professional memberships
- Health information
- Documents in case of disciplinary matters, e.g. warnings.

3.2.2 In your employee file we also store your application, employment contract and other relevant information about your employment relationship.

3.2.3 It is essential that appropriate changes to this data are recorded and it is imperative that you, as an employee, advise your line manager of any changes to the data we may hold.

3.2.4 There may also be situations where we handle information that is not listed in the list above.

3.2.5 We may collect and process personal data for the following purposes:

- To ensure necessary and relevant information in relation to the performance of the individual employment and to comply with any law, rule, regulation, lawful and binding determination, decision or direction of a regulator, or in co-operation with any governmental authority of any country (e.g. GDPR), including:
- Documentation requirements
- Compliance with legal obligations and best practice principles for processing of personal data
- Implementation and maintenance of technical and organizational security measures, including but not limited to, preventing unauthorized access to systems and information, prevent receipt or distribution of malicious code, termination of denial-of-service-attacks and damage to computer systems and electronic communication systems
- Investigation of suspected or known security breaches and reporting of such breach to individuals and authorities
- To process and respond to requests and complaints from data subjects and others
- Handling of inspections and requests from authorities

- Management of disputes with data subjects and third parties.

3.3. Automated, individual decision making

3.3.1 Personal data is not used for automated, individual decision making or profiling.

3.4. The legal basis for processing the personal information

3.4.1 The legal basis for processing of general and sensitive personal data as outlined above is the employment contract (cf. article 6(1)(b))

3.4.2 The legal basis for processing potential personality tests are is consent (cf. article 6(1)(a))

3.4.3 The personal information collected about you or employment purposes supports our contracts with you as our employees.

3.4.4 Please refer to the Checklist - Legal basis for processing personal data in our GDPR Policy

3.5. Disclosure of personal information

3.5.1 Personal information collected by Falck UK will be disclosed to and shared with the following recipients:

- Government departments and tax authorities
- External and internal audit
- Pension funds, banks and insurance companies

3.6. Special category data

3.6.1 We will pay particular regard to the security of personal data defined as special category data under GDPR, which may include:

- race
- ethnic origin
- politics
- religion
- trade union membership
- genetics
- biometrics (where used for ID purposes)
- health
- sex life
- sexual orientation.

3.7. Transfer of personal information to data processors

3.7.1 We transfer your personal data to certain suppliers, e.g. IT suppliers, who process the information on behalf of Falck.

3.7.2 Transfer of personal data to recipients in countries outside European Union (EU)/European Economic Area (EEA)

3.7.3 We transfer your data to recipients in countries outside EU/EEA as we use an external supplier to host/store the above mentioned personal information. The basis for the international transfer is EU's "Standard Contractual Clauses" for transfers from data controllers to data processors in countries without an adequate level of protection outside EU/EEA. The standard agreement is available in different languages via this link: http://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1401799946706&uri=CELEX:32010D0087.

3.7.4 Please refer to the Checklist - International transfers of personal data in our GDPR Policy

3.7.5 Further information about data providers and transfers to recipients outside the EU/EEA can be obtained from the Human Resources department (hr.team@medicalservicesuk.com).

3.8. Retention periods

3.8.1 We retain your personal data as long as necessary, in accordance with NHS defined retention periods ( https://digital.nhs.uk/records-management-code-of-practice-for-health-and-social-care-2016) in order to fulfill the above stated purposes. It is acknowledged that the code of practice and related retention period schedule is currently under review and our practices will be amended to reflect the new code of practice once published.

3.9. Contact details

3.9.1 If you have any questions or comments with respect to the processing of your personal data or you wish to exercise your rights under applicable legislation, please contact Lezli Feeney, Head of Health Safety Environment and Quality [lezli.feeney@medicalservicesuk.com]. Support in responding to you request will be provided by the Director of Human Resources and our IT services provider. You may also our global group data protection officer by emailing to dpo@falck.com or writing to:

Falck [Danmark] A/S

Polititorvet 1

1780 København V

Date: 18 April 2018

## 4) Related policies/procedures

*Information Governance Policy*
General Data Protection Regulation (GDPR) Policy
*Information Security Policy and all other IT policies*
*Clinical Records Policy*
*Records Management Policy*
*Registrations Policy*
*Social Media Policy*
*Whistleblowing Policy*

## 5) References

EU GDPR Portal (2018) *Site overview* [online] https://www.eugdpr.org/

NHS Digital (2016) *records management code of practice* [online] https://digital.nhs.uk/records-management-code-of-practice-for-health-and-social-care-2016

## 6) Appendices

18908 Registrations Policy including Complaints, Incident Reporting, Significant Events and Serious Incidents and Duty of Candour
19125 Information Governance Policy
20535 Whistleblowing UK Policy
37611 Misuse of Social Media
38092 Records Management Policy including Clinical Records
Chapter: Falck UK Ambulance Service Ltd - 3. 5.1 Policy/Procedure

**Version history**

| Version | Approval | Revision information |
|---|---|---|
| 1 | 30.05.2018 | |
| 1.0 | 16.10.2018 | |