NHS
Business Services Authority

Statement of Data Protection Roles and Responsibilities

Purpose

This statement sets out the roles and responsibilities of the NHS Business Services Authority (NHSBSA) under Data Protection Legislation as it relates to the NHS Electronic Staff Record Service (ESR).

The NHSBSA will not enter into individual agreements for data protection with NHS Employing Authorities who use ESR. This statement coupled with the use of ESR gives effect to the data processing relationship between the parties.

This statement meets the requirements of Data Protection Legislation and sets out the following: -

- Roles of the NHSBSA and an NHS Employing Authority
- The legal basis for processing
- The subject matter processed
- The duration of the processing
- The type and categories of personal data held and processed
- The responsibilities for Data Subject Rights Requests
- The process for handling breaches
- The process for attributing liabilities

Please note the terms used in this statement are defined in the definitions section at the end of this document.

NHSBSA ESR and NHS Employing Authorities

The ESR and the Employing Authorities have the following roles, as defined by Data Protection Legislation: -

Party	**Role**
NHSBSA	Joint Controller
NHS Employing Authority	Joint Controller

NHSBSA ESR and NHS Employer Responsibilities

The Joint Controllers have the responsibilities detailed in the table below to comply with the GDPR Article 26 transparency requirement: -

Responsibility	**Details**
Determine the legal basis of processing (GDPR Article 6)	<u>NHSBSA ESR:</u> GDPR Article 6(1)(c) necessary for compliance with legal obligations and Data Protection Act (DPA) 2018 section 10 and the Applied GDPR Article 9(2)(g) as inserted by DPA 2018 Schedule 6 paragraph 12(c) "*processing is necessary for reasons of substantial public interest and is authorised by domestic law.*" <u>Employing Authority:</u> The NHSBSA understands that the NHS Employers has the following legal basis: GDPR Article 6(1)(b) necessary for the performance of a contract with the data subject; GDPR Article 9(2)(b) , (h) and (g) and DPA 2018 Section 10(1)(a) necessary for UK employment and social security and social protection law.

Responsibility	Details
Document the subject matter of the Processing (GDPR Article 30 (b))	NHSBSA will manage the contract and service delivery of ESR. The NHS Employing Authorities will maintain employment records relating to their employees data.
Document the duration of the Processing (GDPR Article 30 (f))	NHSBSA will process and store the data as detailed in the ESR Privacy Policy and Data Retention Policy. Beyond the NHSBSA ESR Data Retention Policy periods, NHS Employing Authorities will determine their own duration and retention periods in line with their own policies and procedures.
Document the nature and purpose of the Processing (GDPR Article 30 (b))	The joint controllers will administer and maintain employee records for payroll and workforce planning purposes.
Document the type of Personal Data (GDPR Article 30 (c))	• Family, lifestyle and social circumstances • Financial details • Employment and education details • Equality and Diversity Declarations • Physical or mental health details • Trade Union Membership • DBS check result where applicable
Document the categories of Data Subjects (GDPR Article 30 (c))	• Employees and ex-employees • Next of kin of Employee • Connected Persons • Referees • Medical Practitioner details

Responsibility	Details
Responding to Data Subject Rights Requests: Right of Access (GDPR Article 15) Right to Rectification (GDPR Article 16) Right to Erasure (GDPR Article 17)	NHSBSA will action these rights for the requests it receives from NHS Employing Authorities based on the personal data it holds for NHS Employers who: • no longer exist and • have no organisation with responsibility for them. The NHS Employer will action these rights for the requests it receives and the personal data it holds within ESR. ESR has a report available to designated users to help answer Subject Access requests.
Providing Privacy Notices to Data Subjects (GDPR Articles 13 - 14)	NHSBSA has provided a privacy notice at http://www.esrsupport.co.uk/privacy-2018-05014-v1.php and will be accessible through the ESR self Service portal. The NHS Employer will make their staff aware of the processing they undertake in ESR.
Handling Personal Data Breaches (GDPR Articles 33 - 34)	The ESR Processor will advise the ESR contact within the affected NHS Employing Authority and the NHSBSA designated contacts. Security incidents will be managed by the Processor in accordance with jointly agreed security procedures. The NHS Employing Authority will handle personal data breaches relating to the relevant employee data they hold.
Data Subjects right to compensation and liability (GDPR Article 82)	The NHS Employing Authority will be liable for any compensation claims unless the cause is a result of the acts or omissions of the ESR Processor.

Responsibility	Details
Contact point for Data Subjects (GDPR Article 38)	The Data Protection Officer of the NHS Employing Authority,

Definitions

“Connected Persons”	a person authorised in writing by a Data Subject to act on their behalf; or a person appointed under a valid power of attorney to act on behalf of a Data Subject;
“Controller”	has the meaning given in Data Protection Legislation and "Joint Controllers" has the meaning given in Article 26 GDPR;
"Data Protection Legislation"	the Data Protection Act 2018 (DPA), the General Data Protection Regulation (Regulation (EU) 2016/679 of the European Parliament and of the Council (GDPR), the Regulation of Investigatory Powers Act 2000, the Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000, the Electronic Communications Data Protection Directive 2002/58/EC, the Privacy and Electronic Communications (EC Directive) Regulations 2003 and all applicable laws and regulations relating to Processing of Personal Data and privacy, including where applicable the guidance and codes of practice issued by the Information Commissioner;
“Data Subject”	has the meaning given in Data Protection Legislation;
“Data Subject Rights Request”	a request made by a Data Subject in accordance with rights granted pursuant to Data Protection Legislation to access his or her Personal Data as set out in Articles 15 to 22 of GDPR;
“European Law”	European Union or European Member State law (as referred to in the GDPR) or such other law as may be designated in its place when England (whether with Scotland, Wales and/or North Ireland or not), leaves the European Union;
"GDPR"	the General Data Protection Regulation (Regulation (EU) 2016/679 of the European Parliament and of the Council);
"Personal Data"	has the meaning given in Data Protection Legislation;

“Process”	has the meaning given in Data Protection Legislation and “Processed” and “Processing” shall be construed accordingly;
“Processor”	has the meaning given in Data Protection Legislation;