East Sussex County Council Special Category Data Policy

Summary

This policy outlines the Council's obligations under Data Protection Legislation with regard to the processing of Special Category Personal Data.

1. Policy Statement

East Sussex County Council is committed to ensuring that all personal data it processes, is managed appropriately and in compliance with the General Data Protection Regulation (GDPR) and the Data Protection Act 2018 (DPA 2018) (collectively referred to as "DP legislation").

The Council recognises its duties to protect all personal data but in particular Special Category Personal Data as defined under Data Protection legislation i.e. information that may identify an individual's:

- racial or ethnic origin,
- political opinions,
- religious or philosophical beliefs,
- trade union membership,
- health,
- sex life/orientation
- genetic/biometric identifier
- criminal convictions/offences

Heads of Service/Information Asset Owners will ensure that all Special Category Data is captured, held or used in their business area in compliance with this policy. Any proposed new use of Special Category Data will be subject to a Data Protection Impact Assessment.

For all uses of Special Category Data, the processing will be included in the Council's Record of Processing Activity (ROPA). This will include a description of the lawful basis for processing and confirmation that the appropriate data retention rules are being applied.

Failure to comply with this policy may be subject to disciplinary procedures.

2. Responsibilities

- The **Senior Information Risk Officer (SIRO)** has overall responsibility for ensuring compliance with this policy and with DP legislation;
- The **Data Protection Officer (DPO)** has responsibility for advising the organisation on data protection matters, and for monitoring compliance with this policy.
- **Heads of Service/Information Asset Owners** are responsible for ensuring that all systems, processes, and information assets within their business area are compliant with this policy and with DP legislation.

- **All staff** are responsible for understanding and complying with relevant policies and procedures for protecting special category and criminal conviction data.

3. Related Documents

- Information Security/Data Protection Policy
- Record of Processing Activity (Information Asset Register)
- Information Security Incident Policy
- Data Protection – Guidance for Employees
- Case Recording Policy

4. Compliance with the Principles

All processing of personal data, including Special Category Data, is subject to the Councils Information Security/ Data Protection Policy and all related procedures for data handling. Below is a summary of our procedures for compliance with the principles under Article 5 of GDPR.

Data Protection Principle	Procedures for securing compliance	Relevant policies/procedures
Personal data will be processed lawfully, fairly and in a transparent manner	All use of Special Category Data will be: Assessed for lawfulness, fairness and transparency as part of Data Protection Impact Assessments (DPIA). described clearly and precisely in privacy notices available to data subjects. The Council will ensure that personal data is only processed where a lawful basis applies, (i.e. is subject to clear justification under Article 6 and 9 of GDPR). The Council will only process personal data fairly, and will ensure that data subjects are not misled about the purposes of any processing.	Information Security/ Data Protection Policy. Data Protection – Guidance for Employees.
Personal data will be collected and used for specified, explicit and legitimate purposes and not	(This will be checked within the DPIA process). Staff will be trained to ensure that they do not use personal data for	Information Security/Data Protection Policy.

Data Protection Principle	Procedures for securing compliance	Relevant policies/procedures
further processed in an incompatible way ('purpose limitation')	purposes other than those authorised by the organisation. Staff will receive training and document procedures for relevant processes. Data subjects will be informed of the purpose for processing in a privacy notice.	Record of Processing Activity/Information Asset Register. Mandatory IG/DP Training. Data Protection – Guidance for Employees.
Personal data collected and processed will be adequate, relevant and limited to what is necessary for the purpose for processing ('data minimisation')	All forms and systems are subject to Data Protection by Design controls to ensure only data relevant to the business requirement is captured, held and made available. Our systems have roles-based access and staff will be trained to record only the minimal necessary personal data for business needs. (This will be checked within the DPIA process.)	Information Security/ Data Protection Policy. Data Protection – Guidance for Employees.
Personal data will be accurate and where required, rectified without delay ('accuracy')	Data accuracy verified using system controls (where applicable) and staff responsible for ensuring accuracy of data recording. (This will be checked within the DPIA process.)	Information Security/ Data Protection Policy. Data Protection – Guidance for Employees. Case Recording Policy.
Personal data will not be kept in an identifiable form for longer than necessary ('storage limitation') i.e. in line with Council retention schedules	Heads of Service are tasked with ensuring that the Records Retention Schedule is applied to all personal data, and in particular to Special Category Data. Where systems do not have the functionality to automate disposal, staff have a scheduled task to manually delete time-expired data.	Information Security /Data Protection Policy. Data Protection – Guidance for Employees. Records Retention Schedule.
Personal data will be kept securely	All use of personal data is subject to our Information Security and Data Protection Policy and related controls. Staff are trained to be particularly aware of the additional risks to Special Category Data and the relevant teams have appropriate data-handling processes and guidance.	Information Security/ Data Protection Policy. Data Protection – Guidance for Employees

Data Protection Principle	Procedures for securing compliance	Relevant policies/procedures
	Appropriate means of transmitting data are used. Data is securely stored and securely disposed of (where retention periods are reached) Where processing is sub-contracted or outsourced there are suitable Data Protection clauses in the contract.	

Contact

If you have any questions about this policy, please contact:

By Post:
Data Protection Officer
County Hall
St. Anne's Crescent
Lewes
East Sussex
BN7 1UE

By Email: DPO@eastsussex.gov.uk

Document Title: Special Category Data Policy.
Version Number: 1.0.
Document Approved By: Senior Information Risk Owner.
Approval date: 15 February 2019.
Review date: 15 January 2020.
Version History: None.
Security Classification: Official Disclosable.

This policy is subject to review annually. Superseded policies will be retained for at least 6 months.