Nottinghamshire Police Record of Processing Activities (RoPA)

Introduction

The introduction of the General Data Protection Regulations (EU) 2016/679 and the UK Data Protection Act 2018 introduced significant changes to the responsibilities of organisations that collect, store and share personally identifiable information. Nottinghamshire Police are fully committed to full compliance with the requirements of this legislation including that connected to the recording of our processing activities.

Nottinghamshire Police needs to collect and use information about people with whom it works in order to operate and carry out its functions. These may include members of the public, current, past and prospective employees, suspects, offenders, witnesses, information providers, suppliers, and people who use our services. This Personal Data must be handled and dealt with properly however it is collected, recorded and used and whether it is on paper, in computer records or recorded by other means.

In order to ensure we understand the processing activities in respect of Personal Data within Nottinghamshire Police, we have completed the following Record of Processing Activities (RoPA).

In addition you can also obtain further information by contacting the Data Protection Officer, sending an email to data.protection@nottinghamshire.pnn.police.uk or looking at the Information Commissioner's Website at ICO.org.uk.

The name and contact details of the controller/processor and, where applicable, the joint controller, the controller's/processor's representative and the data protection officer	Controller and Joint Controller The Chief Constable, Nottinghamshire Police, Headquarters, Sherwood Lodge, Arnold, Nottingham, NG5 8PP. DPO Pat Stocker, Information Management Unit, Nottinghamshire Police, Headquarters, Sherwood Lodge, Arnold, Nottingham, NG5 8PP. Email: data.protection@nottinghamshire.pnn.police.uk Deputy DPO Lehan Fielding, Information Management Unit, Nottinghamshire Police, Headquarters, Sherwood Lodge, Arnold, Nottingham, NG5 8PP. Email: data.protection@nottinghamshire.pnn.police.uk

The purposes of the processing:	Nottinghamshire Police process data for Law Enforcement purposes in our role as a Police Force (Competent Authority), which includes the following categorisation of individuals: • Suspects • Offenders • Victims • Witnesses • Request for Assistance • Information Providers Nottinghamshire Police also process data for General Processing in our role as Police Force which includes: • Supporting network and system security; • Auditing; • Complying with legal obligations; and • Conducting web analytics. • Recruitment and selection of employees; • Personnel management; • Workplace monitoring; • Human resources administration including payroll and benefits; • Education, training and development activities. • To obtain products and services; • Vendor administration, order management and accounts payable; and • Evaluating potential suppliers. • Members of the public who use our website • Members of the public who write to NOTTINGHAMSHIRE POLICE via the public website • Third parties we may communicate with where we do not have a contract Please refer to the Force Information Asset Register for a full list of our Processing Activities.
Categories of data subjects:	Nottinghamshire Police process the following types of data subjects for both Law Enforcement and General Processing which includes the following categorisation of individuals:

	• Suspects • Offenders • Victims • Witness • Requests for assistance • Information providers • Employees • Suppliers • Successful and Unsuccessful employment candidates • People who use our services or the services we provide on behalf of others
Categories of personal data: -	Nottinghamshire Police process the following types of data categories for both Law Enforcement and General Processing which includes: • Personal details including name and contact information • Date of birth • Gender • Marital status • Biometric information • Beneficiary & emergency contact Information • Family and lifestyle details • Government identification numbers • Education and training details • Bank account details and payroll information • Wage and benefit information; • Performance information • Employment details. • Device details • User activity • Browser history details • Location details • Electronic identification data including IP address • Financial details • Payment details • Contractual details including the goods and services provided; and • Name & contact information of suppliers • Callers • Visitors records

	<u>Special categories of (sensitive) personal data:</u> The special categories specifically include genetic data, and biometric data where processed to uniquely identify an individual: • Race • Ethnic origin • Politics • Religion • Trade union membership • Genetics • Biometrics (where used for ID purposes) • Health • Sex life; or • Sexual orientation.
The categories of recipients to whom the personal data have been or will be disclosed including recipients in third countries or international organisations	Nottinghamshire Police will disclose and share information that it processes for both Law Enforcement and General Processing with the below which includes: ● Disclosures to other law enforcement agencies (including international agencies and those involved in National Security) ● Partner agencies working on crime reduction initiatives ● Partner Agencies involved in the Safeguarding of Children and Vulnerable Adults ● Partners in the Criminal Justice arena, ● Victim Services, and ● Local government ● Central government ● Ombudsmen and regulatory authorities ● The Media ● Other bodies or individuals where necessary to prevent harm to individuals ● HM Revenue and Customs ● licensing authorities ● legal representatives ● prosecuting authorities ● defense solicitors ● courts ● prisons ● partner agencies involved in crime and disorder strategies

	• private sector organisations working with the police in anti-crime strategies • voluntary sector organisations • approved organisations and people working with the police • Independent Police Complaints Commission • Her Majesty's Inspectorate of Constabulary • Auditors • Office of Police & Crime Commissioner
Where applicable, transfers of personal data to a third country or an international organization, including the identification of that third country or international organization and, in the case of transfers referred to in the second subparagraph of Article 49(1), the documentation of suitable	Nottinghamshire Police will transfer personal data to: • Niche (Canada) – any data is encrypted prior to transfer and is destroyed by Niche when they have completed their testing. • Interpol – any data transferred has an adequate level of protection and/or is necessary for Law Enforcement purposes. • Other International Law Enforcement Bodies- any data transferred has an adequate level of protection and/or is necessary for Law Enforcement purposes.
Where possible, the envisaged time limits for erasure of the different categories of data	• Nottinghamshire Police adhere to the Regional Review, Retention & Deletion (RRD) Policy for Niche information managed by the Regional RRD Team at Lincolnshire Police under MoPI guidance. • For other information processed by the Force, Nottinghamshire Police adhere to the National Retention Schedule provided by NPCC IMORCC. Please see the Information Asset Register for details regarding the retention periods of specific information
Where possible, a general description of the technical and organisational security measures referred to in Article 32(1) - *Anonymisation of personal data;* - *Encryption of personal data;*	All access to information whether digital or paper is managed by role based access controls, Active Directory authentication including passwords, privilege levels, physical security, printer passwords, shredding facilities

- *Segregation of personal data from other networks;* - *Access control and user authentication;* - *Employee training on information security; and* - *Written information security policies and procedures.*	and services, secure disposal of hardware assets and electronic and physical door access controls. All aspects outlined above are described in detail within Force policies. Like all Forces, Nottinghamshire must gain an annual compliance certificate in order to access the Public Services Network. There is a strict code of connection, which outlines mandatory controls such as secure configuration, physical security, protective monitoring, authentication and boundary protection. In addition to PSN compliance, there is an additional code of connection to connect to PSN (P), the encrypted police overlay providing access to National systems called the Governance & Information Risk Return (GIRR). The GIRR covers additional controls such as mobile device configuration, data encryption in transit, asset management, and access control and network security. All the above being compliant to nationally agreed standards. All new systems are accredited before they go live. This ensures that any risk to the confidentiality, integrity and availability of data is documented and mitigated where possible and in line with the Senior Information Risk Officer (SIRO), Information Risk Appetite. All Nottinghamshire Policing purpose systems and those containing personal information have a dedicated Information Asset Owner, who receive training to ensure that that they understand their role and responsibilities in accordance with the Force Information Assurance Strategy. With this including their management of who has access to the systems they are each responsible All individuals with direct access to Nottinghamshire Police information assets are required to complete mandatory annual Data Protection and Information Security training to ensure that they are aware of their

	responsibilities. There is a Force Information Security Policy in place, which is published on the Force Intranet and regular security reminders are also published.