Record of Processing Activities Under Article 30 (GDPR)

This Record of Processing Activities (Record) describes how the National Association of Retired Police Officers (NARPO) processes personal data. NARPO recognizes that Article 30 of the EU General Data Protection Regulation (GDPR) imposes documentation requirements on controllers and processors of data. This Record is company confidential information but NARPO will provide it to the appropriate supervisory authority on request as required by Article 30.

Data Controller Details:

Name: National Executive Committee, NARPO

Address: 38 Bond Street, Wakefield, WF1 2QP

Telephone Number: 01924 362166

Website: www.napro.org

Joint controller: Branch Officials of each Branch of NARPO

Data Protection lead: Alan Lees, National Association of Retired Police Officers, 38 Bond Street, Wakefield, WA1 2QP. Email depceo@narpo.org

Data Protection Officer – the NEC have appointed an external organisation to fill this role and this is Affinity Resolutions.

Categories of Data Subjects

NARPO collects personal data from the following categories of data subjects:

1. NARPO members.
2. NARPO vendors and suppliers.
3. NARPO employees and job applicants.

Categories of Personal Data

NARPO collects the following categories of personal data about members:

1. Personal details including name and contact information.
2. Family and lifestyle details.
3. Device details.
4. User activity details and user preferences.
5. Browser history details.
6. Location details.
7. Electronic identification data including IP address and information collected through cookies.
8. Financial details.
9. Credit card information and payment details.
10. Contractual details including the goods and services provided.
11. Photographs.
12. Special categories of personal data including biometric data.

NARPO collects the following categories of personal data about employees and job applicants:

1. Personal details including name and contact information.
2. Date of birth.
3. Gender.
4. Marital status.
5. Beneficiary and emergency contact information.
6. Government identification numbers.
7. Education and training details.
8. Bank account details and payroll information.
9. Wage and benefit information.
10. Performance information.
11. Employment details.
12. Photographs.

13. Special category data including data on health.

NARPO collects the following categories of personal data about vendors and suppliers:

1. Name and contact information.
2. Financial and payment details.

Purposes of Data Processing

NARPO collects and processes personal data about members for the following purposes:

1. Welfare of members.
2. Maintaining and enhancing NARPO's products and services.
3. Providing products and services and customer management.
4. Account management.
5. Direct marketing.
6. Supporting network and system security.
7. Auditing.
8. Detecting and preventing fraud.
9. Complying with legal obligations.
10. Conducting web analytics.

NARPO collects and processes personal data about employees and job applicants for the following purposes:

1. Recruitment and selection of employees.
2. Personnel management.
3. Workplace monitoring.
4. Human resources administration including payroll and benefits.
5. Complying with legal obligations.
6. Education, training, and development activities.

NARPO collects and processes personal data about vendors and suppliers for the following purposes:

1. To obtain products and services.
2. Vendor administration, order management, and accounts payable.
3. Evaluating potential suppliers.
4. Detecting and preventing fraud.

NARPO having considered the lawful basis for processing records:

1. Consent – brought to the attention of the data subject on the first occasion engages with them.
2. Contract – brought to the attention of the data subject on the first occasion engages with them and in the privacy policy.
3. Legal obligation – brought to the attention of the data subject on the first occasion engages with them and in the privacy policy.
4. Legitimate interests – brought to the attention of the data subject on the first occasion engages with them and in the privacy policy.

Categories of Personal Data Recipients

NARPO may be required to discloses personal data to the following categories of recipients, some of which may be located in third countries or may be international organizations as defined in Article 4(26) of the GDPR:

1. NARPOs branches.
2. Business partners when required by a member.
3. Auditors and professional advisors, such as lawyers and consultants.
4. State, and local law enforcement officials.
5. Third-party service providers, such as providers of:
    - IT system management;
    - Information security;
    - Human resources management;
    - Payroll administration; or
    - Retirement plan administration.

Transfer of personal data to third countries and international organisations.

NARPO makes limited personal data transfers subject to the second subparagraph of Article 49(1) which are necessary for NARPOs compelling legitimate interests. NARPO provides appropriate safeguards for these limited personal data transfers through contractual clauses.

Data Registers

NARPO retains the following registers:

1. Access request register.
2. Personal data breach register.
3. Data impact assessment register.
4. Register of contracts with processors and copies of contract.
5. Register of assessment and review of data protection policies and procedures.

Personal Data Retention Periods

Except as otherwise permitted or required by applicable law or regulation, NARPO only retains personal data for as long as necessary to fulfil the purposes NARPO collected it for, as required to satisfy any legal, accounting, or reporting obligations, or as necessary to resolve disputes. To determine the appropriate retention period for personal data, NARPO considers the amount, nature, and sensitivity of personal data, the potential risk of harm from unauthorized use or disclosure of personal data, the purposes for processing the personal data, whether the employer can fulfil the purposes of processing by other means, and any applicable legal requirements.

NARPO typically retains personal data for the periods set out below, subject to any exceptional circumstances or to comply with laws or regulations that require a specific retention period:

Information about members – the period of retention is normally two years after ceasing to be a member:

- personal details including name and contact information: two years;
- family and lifestyle details: two years;
- device details: two years;
- user activity details and user preferences: two years;
- browser history details: two years;
- location details: two years;
- electronic identification data including IP address and information collected through cookies: two years;

- contractual details including the goods and services provided: two years.
- when a Member is convicted of a criminal offence or dismissed from a Branch: indefinitely.

Information about employees and job applicants – the period of retention is normally six years after ceasing to be an employee:

- personal details including name and contact information: six years;
- date of birth: six years;
- gender: six years;
- marital status: six years;
- beneficiary and emergency contact information: six years;
- government identification numbers: six years;
- education and training details: six years;
- bank account details and payroll information: six years;
- wage and benefit information: six years;
- performance information: six years;
- employment details: six years;
- special categories of personal data, including information that relates to an employee's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, genetics or health, and sex life or sexual orientation: six years.

Information about vendors or suppliers – the period of retention is after the end of end contract period:

- name and contact information: six years;
- financial and payment details: six years.

Technical and Organizational Security Measures

NARPO has implemented the following technical and organisational security measures to protect personal data:

1. Segregation of personal data from other networks.
2. Access control and user authentication.
3. Employee training on information security.
4. Written information security policies and procedures.

Changes to this Record of Processing Activities

NARPO reserves the right to amend this Record of Processing Activities from time to time consistent with the GDPR and other applicable data protection requirements.

Effective Date:

15.5.2018

Last modified:

15.5.2018