nipsa

Protecting Public Services
Supporting Public Servants

Data Protection Policy

May 2018

1. Policy Statement

1.1 NIPSA is committed to compliance with all relevant EU and UK laws in respect of personal data, and the protection of the rights and freedoms of individuals whose information we collect and process in accordance with the General Data Protection Regulation (GDPR). We are registered with the Information Commissioner's Office (ICO) as a Data Controller for the personal data that we hold and process.

1.2 Everyone has rights regarding the ways in which their personal data in handled. The importance of keeping members'/staff affairs confidential, protecting personal and sensitive personal data and keeping information secure is fundamental. This policy is designed to cover all these areas so that all "agents of NIPSA" (the Unions' Officers, staff, activists and members etc.) are clear about their obligations and how to protect data/ensure confidential information is kept confidential. This policy applies to all "agents of NIPSA" (the Unions' Officers, staff permanent and temporary, activists and members, agency, and contract staff). Any breach of the GDPR may be dealt with under our disciplinary policy and may also be a criminal offence, in which case the matter will be reported as soon as possible to the appropriate authorities. In addition to the requirement of adhering to these policy requirements and NIPSA rules, non-NIPSA staff are also subject to the legitimate fulfilment of their employer's statutory Data Protection duties.

1.3 Third parties working with us, or for us, which have or may have access to personal data will be expected to adhere to all obligations imposed by data protection legislation. No third party may access personal data held by us without having first entered into a Data Sharing Agreement which imposes on the third party obligations no less onerous than those to which we are committed, and which gives us the right to audit their compliance with the Data Sharing Agreement.

1.4 **The Deputy General Secretary of NIPSA or in their absence the General Secretary of NIPSA is the Data Protection Officer (DPO) and is responsible for all data protection matters.**

2. About This Policy

2.1 The types of personal data that NIPSA may be required to handle includes information about current, past and prospective members'/staff suppliers, Third Parties and others with whom we communicate. The personal data, which may be held on paper, on a computer or other media, is subject to certain legal safeguards specified in the GDPR. The lawful basis for processing; type of information held; use of information; detail of with whom it is shared as well as members'/staff rights in relation to their personal data is detailed in our privacy notice (See Appendix 1).

2.2 We reserve the right to change this policy at any time. Should this policy be changed/updated, branches will be notified of this fact and the updated policy posted on the NIPSA website.

3. Definition of Data Protection Terms

Child – the GDPR defines a child as anyone under the age of 16 years. The processing of personal data of a child is only lawful if parental or custodian consent has been obtained. The data controller shall make reasonable efforts to verify in such cases that consent is given or authorised by the holder of parental responsibility over the child.

Consent - means any freely given, specific, informed, and unambiguous indication of the Data Subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data.

Data is information which is stored electronically, on a computer, or in certain paper-based filing systems.

Data breach – a breach of security leading to the accidental, or unlawful, destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored, or otherwise processed. The data controller is required to report data breaches to the Information Commissioner's Office (ICO), particularly breaches likely to adversely affect the personal data or privacy of the Data Subject.

Data Controller – the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by EU or Member State law, the Data Controller or the specific criteria for its nomination may be provided for by EU or Member State law.

Data Processor - in relation to personal data, means any person (other than an employee of the data controller) who processes the data on behalf of the data controller.

Data Subject – any living individual who is the subject of personal data held by an organisation.

Data users are those of our employees whose work involves processing personal data. Data users must protect the data they handle in accordance with this data protection policy and any applicable data security procedures at all times.

Personal data – any information relating to an identified or identifiable natural person (**'Data Subject'**); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

Processing – any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

Sensitive Personal Data – personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade-union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a living person, data concerning health or data concerning a living person's sex life or sexual orientation.

Third Party – a natural or legal person, public authority, agency or body other than the Data Subject, data controller, data processor and persons who, under the direct authority of the data controller or data processor, are authorised to process personal data.

4. Data Protection Principles

All processing of personal data must be conducted in accordance with the Data Protection Principles as set out in the GDPR and outlined below. Our policies and procedures are designed to ensure compliance with these Principles.

Principle 1

Personal data must be processed lawfully, fairly, and transparently

Lawfully– we need to identify a lawful basis before we can process personal data e.g. consent.

Fairly – in order for processing to be fair, we have to make certain information available to Data Subjects. This applies whether the personal data was obtained directly from Data Subjects or from other sources.

Transparently – the GDPR includes rules on giving privacy information to Data Subjects. These are detailed and specific, placing an emphasis on making privacy notices understandable and accessible. Information must be communicated to the Data Subject in an intelligible form using clear and plain language.

Principle 2

Personal data can only be collected for specific, explicit, and legitimate purposes
The data we obtain for specified purposes must not be used for a purpose that is incompatible with those purposes.

Principle 3

Personal data must be adequate, relevant, and limited to what is necessary for processing
We cannot collect information that is not strictly necessary for the purpose for which it is obtained.

Principle 4

Personal data must be accurate and, where necessary, kept up to date.
Every reasonable step must be taken to ensure that personal data we hold is accurate and up to date. Data that is stored by us must be reviewed and updated as necessary. No data should be kept unless it is reasonable to assume that it is accurate. Reasonable steps must be taken to destroy or amend inaccurate or out-of-date data.

Principle 5

Personal data must be kept in a form such that the Data Subject can be identified only as long as is necessary for processing.
We should only keep personal data for as long as we need it. We will take all reasonable steps to destroy, or erase from our systems, all data which is no longer required.

Principle 6

Personal data must be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures
We will put in place procedures and technologies to maintain the security of all personal data from the point of collection to the point of destruction.

5. Demonstrating Accountability

The GDPR includes provisions that promote Accountability and Governance. These complement the GDPR's transparency requirements. Accountability requires us to demonstrate that we comply with the GDPR Principles.

We will demonstrate compliance with the GDPR Principles by implementing and adhering to data protection policies, implementing technical and organisational measures, as well as adopting techniques such as Data Protection by Design, Data Protection Impact Assessments, breach notification procedures and incident response plans.

6. Data Subjects' Rights

The GDPR provides the following rights for individuals in relation to their personal data:

1. The right to be informed
2. The right of access
3. The right to rectification
4. The right to erasure
5. The right to restrict processing
6. The right to data portability
7. The right to object
8. Rights in relation to automated decision making and profiling.

Data Subjects may make Subject Access Requests relating to their personal data.

Our DPO is responsible for responding to requests for information from Data Subjects within one calendar month. This can be extended to two months for complex requests in certain circumstances. If we decide not to comply with the request, the DPO must respond to the Data Subject to explain our reasoning and inform them of their right to complain to the ICO and seek judicial remedy.

Data Subjects have the right to complain to us about the processing of their personal data, the handling of a Subject Access Request and to appeal against how their complaints have been handled.

7. Lawful Basis for Processing Data and Consent

Under GDPR, as a "data controller" we can choose a number of lawful bases for the processing of data, with no hierarchy signified by the choice and, potentially, different bases used for different activities, "**Legitimate Interests"** is the most appropriate for NIPSA in that our members in relation to their membership/participation in the work of the Union would have a "reasonable

expectation" that: we will process their personal data and such processing will not be unexpected or unwanted. For certain NIPSA activity beyond basic membership i.e. for activists, nominees for office, committee members etc. we will seek their consent to be contacted by NIPSA for the purpose of this activity; for their personal data to be retained by NIPSA for this purpose and for this data be deleted when the specific activity has ceased/come to an end (i.e. end of term of office of Committee or the end of a campaign etc.). (See Appendix 2 Consent Form for Activists/Nominees/Committee Members)

We understand 'consent' to mean that it has been explicitly and freely given, and it is a specific, informed and unambiguous indication of the Data Subject's wish that, by statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her. The Data Subject can withdraw their consent at any time. We also understand 'consent' to mean that the Data Subject has been fully informed of the intended processing and has signified their agreement while in a fit state of mind to do so and without pressure being exerted upon them. Consent obtained under duress or on the basis of misleading information will not be a valid basis for processing.

8. Collection of Data

All data collection forms (electronic and paper-based), including data collection requirements in new information systems, must include a fair processing statement or a reference/link to our Privacy Notice and be approved by the DPO/General Secretary.

9. Accuracy of Data

Our DPO is responsible for ensuring that all employees and "agents of NIPSA" are trained in the importance of collecting accurate data and maintaining it.

Employees are required to notify their employer of any changes in their personal circumstances which may require personal records be updated accordingly.

Our DPO is responsible for ensuring that appropriate procedures and policies are in place to keep personal data accurate and up to date, taking into account the volume of data collected, the speed with which it might change and any other relevant factors.

Our DPO is responsible for making appropriate arrangements where third-party organisations may have been passed inaccurate or out-of-date personal data to inform them that the information is inaccurate and/or out of date and is not to be used to inform decisions about the individuals concerned; and for passing any correction to the personal data to the third party where this is required.

10. Security of Data

All personal data should be accessible only to those who need to use it. All personal data should be treated with the highest security; processed on the basis outlined in our Privacy Notice and adhere to the procedures/instructions re security/retention/disposal of our Data Security Policy. (See Appendix 3).

All requests to provide personal data must be supported by appropriate paperwork and all such disclosures must be specifically authorised by the Data Protection Officer.

We must ensure that personal data is not disclosed to unauthorised third parties, which includes family members, friends, government bodies, and, in certain circumstances, the Police. All employees should exercise caution when asked to disclose personal data held on another individual to a third party.

No less than annually our DPO will carry out a risk assessment taking into account all the circumstances of our data controlling and processing operations.

In determining appropriateness of all technical and organisational security measures, the DPO will consider the extent of possible damage or loss that might be caused to individuals (e.g. staff or members) if a security breach occurs, the effect of any security breach on our organisation itself, and any likely reputational damage, including the possible loss of client trust.

It is strictly prohibited to remove personal data from our premises for any reason other than carrying out legitimate processing activities.

Processing of personal data 'off-site' presents a potentially greater risk of loss, theft, or damage to personal data and the precautions that must be taken are set out in our Data Security Policy.

All employees are responsible for ensuring that any personal data that we hold and for which they are responsible is kept securely and is not, under any condition, disclosed to any third party unless that third party has been specifically authorised by us to receive that information and has entered into a Data Sharing Agreement.

11. Retention and Disposal of Data

We shall not keep personal data in a form that permits identification of Data Subjects for a longer period than is necessary in relation to the purpose(s) for which the data was originally collected.

Personal data will be retained in line with our Data Security (Retention and Disposal) Policy and, once its retention date is passed, it must be securely destroyed as set out in this policy.

On at least an annual basis, our DPO will review the retention dates of all the personal data processed by our organisation and will identify any data that is no longer required. This data will be securely archived, deleted or destroyed in line with our Retention and Disposal Policy.

Our DPO must specifically approve any data retention that exceeds the retention periods defined in our Data Security (Retention and Disposal) Policy, and must ensure that the justification is clearly identified and recorded.

12. International Data Transfers

Under GDPR transfers of personal data outside of the European Economic Area can only be made if specific safeguards exist.

No employee is authorised to transfer personal data internationally until the DPO has confirmed in writing that we have appropriate safeguards in place.

13. Data Protection Impact Assessments (DPIA)

Where a type of processing, in particular using new technologies and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of living peoples, we shall, prior to the processing, carry out a Data Protection Impact Assessment (see Appendix 4) of the envisaged processing operations. All DPIAs should be led by or overseen by the DPO. Where, as a result of a DPIA it is clear that we are about to commence processing of personal data that could cause damage and/or distress to the Data Subjects, the decision as to whether or not we may proceed must be referred to senior management for approval to proceed. Our DPO shall, if there are significant concerns, either as to the potential damage or distress, or the quantity of data concerned, refer to the ICO for guidance and advice.

14. Data Breach

When there has been a data protection breach this must be brought to the attention of the DPO or in their absence the General Secretary. The DPO/NIPSA **MUST** notify the supervisory authority – the Information Commissioner's Office (ICO) without undue delay and within 72 hours (if longer than 72 hours, a specific reason will need to be given). Therefore if you are involved in a data breach you should contact your line manager immediately by telephone/email reporting the nature of the breach and written details of how the breach occurred.

Appendix 1

PRIVACY NOTICE

1. We want you to know that when you use our organisation you can trust us with your information. We are determined to do nothing that would infringe your rights or undermine your trust. This Privacy Notice describes the information we collect about you, how it is used and shared and your rights regarding it.

Data Controller

We are registered with the Information Commissioner's Office (ICO) as a Data Controller for the personal data that we hold and process. Our registered address is NIPSA Headquarters, 54 Wellington Park, Belfast, BT9 6DP, our registration number is Z593111X. Our Data Protection Officer (DPO) is the Deputy General Secretary or in their absence the General Secretary.

2. Data Collection

The vast majority of the information that we hold about you is provided to us by yourself when you seek to use our services. We will tell you why we need the information and how we will use it.

Our Lawful Basis for Processing Your Information

3. The General Data Protection Regulation (GDPR) requires all organisations that process personal data to have a Lawful Bases for doing so. The Lawful Bases for processing, identified in the GDPR are:

   The General Data Protection Regulation (GDPR) requires all organisations that process personal data to have a Lawful Basis for doing so. The Lawful Bases for processing, identified in the GDPR are:

   - **Consent i.e. consent** of the data subject;
   - **Contractual** i.e. performance of a **contract** with the data subject or to take steps to enter into a contract ;
   - **Legal Obligation** i.e. compliance with a legal obligation;
   - **Vital Interests** i.e. To protect the vital interests of a data subject or another person
   - **Public Task** i.e. Performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.
   - **Legitimate Interests** i.e. processing is required under the legitimate interests of ourselves, or a third party, except where such interests are overridden by the interests, rights or freedoms of the data subject.

4. Examples of legitimate interests include:

- Where the data subject is a client or in the service of the controller;
- Transmission within a group of undertakings for internal administrative purposes;
- Processing necessary to ensure network and information security, including preventing unauthorised access;
- Processing for direct marketing purposes, or to prevent fraud; and
- Reporting possible criminal acts or threats to public security.

5. Under GDPR, as a "data controller" we can choose a number of lawful bases for the processing of data, with no hierarchy signified by the choice and, potentially, different bases used for different activities, "**Legitimate Interests"** is the most appropriate for NIPSA in that our members in relation to their membership/participation in the work of the Union would have a "reasonable expectation" that: we will process their personal data in line with the trust outlined at Paragraph 1 and such processing will not be unexpected or unwanted.

6. Our **Legitimate Interest** is to represent fully and inform our members in relation to the activities/services of the Union which they have joined and to encourage their fullest participation in these activities/uptake of these services.

7. **We use your information to:**

- Ensure your full entitlement to union membership and services;
- Provide information to members, for example, branch circulars, NIPSA news etc.
- Process or support payments for goods and services;
- Maintain the safety, security and integrity of our services;
- Direct your enquiries to the appropriate part of the Union area/rep/official;
- Make statutory returns as required and for any other purpose for which you gave your consent.

8. We do not use automated decision-making in the processing of your personal data.

9. We collect and process both personal data and special categories of personal data as defined in the GDPR. This includes:

Member /client data

- Name.
- Email(s).
- Phone Number(s).
- Address(es).
- Employment Status.
- Payment or bank details
- Payroll Number
- NI Insurance Number

- Date of birth
- Location details
- Device IP address.

Employee Data

- Name.
- Email (s).
- Phone Number (s).
- Address.
- Payment or bank details.
- Date of birth.
- Family & next-of-kin details.
- Training/Education Records.
- Disciplinary/Grievance Records.
- Sickness Absence/OHS Reports.
- Leave.

10. **We may share your personal data with:**

- Employers.
- Delivery partners.
- Our legal advisors in the event of a dispute or other legal matter;
- Law enforcement officials, government authorities, or other third parties to meet our legal obligations;
- In connection with, or during negotiations of, any merger, sale of company assets, consolidation or restructuring, financing, refinancing, or acquisition of some or all of our business by another company;
- Independent scrutineers for election/industrial action ballot purposes and any other party where we ask you and you consent to the sharing.

Any and all these parties will be expected to adhere to the principles outlined in this Privacy Notice, our Data Protection Policy and any other Data Protection agreements put in place to protect our members' data.

11. We do not transfer any personal data to third countries or international organisations.

12. **We retain your personal data** while you remain a member unless you ask us to delete it. Our Retention and Disposal Policy (copy available on request) details for how long we hold data and how we dispose of it when it no longer needs to be held. We will delete or anonymise your information at your request unless:

- There is an unresolved issue, such as claim or dispute;
- We are legally required to; or

- There are overriding legitimate business interests, including but not limited to fraud prevention and protecting customers' safety and security.

Your Rights

13. The General Data Protection Regulation gives you specific rights around your personal data. For example, you have to be informed about the information we hold and what we use it for, you can ask for a copy of the personal information we hold about you, you can ask us to correct any inaccuracies with the personal data we hold, you can ask us to stop sending you direct mail, or emails, or in some circumstances ask us to stop processing your details. Finally, if we do something irregular or improper with your personal data you can seek compensation for any distress you are caused or loss you have incurred. You can find out more information from the ICO's website http://ico.org.uk/for_the_public/personal_information and this is the organisation that you can complain to if you are unhappy with how we deal with you.

Accessing and Correcting Your Information

14. You may request access to, correction of, or a copy of your information by contacting us at NIPSA, 54 Wellington Park, Belfast, BT9 6DP . You can update your personal data via the Membership Office/our website.

Cookies

15. Cookies are small text files that are stored on your browser or device by websites, apps, online media, and advertisements. We use cookies on our website but users are made aware that they have the ability to consent to their use/amend settings etc. when they log on.

16. **We will occasionally update our Privacy Notice.** When we make significant changes, we will notify you of these through either mail or email or a branch circular. We will also publish the updated Notice on our website.

Appendix 2

CONSENT FORM FOR ACTIVISTS/NOMINEES/COMMITTEE MEMBERS

I the undersigned have agreed to be nominated by my Union to participate in an activity on behalf of NIPSA. The purpose of this agreement is to protect the confidentiality of personal data held by NIPSA in order to fulfil the obligations placed on us by Regulation (EU) 2016/679 of the European Parliament and the Council commonly referred to as the General Data Protection Regulations (GDPR). **Any data processing carried out on behalf of NIPSA is done on the legal basis outlined in our Privacy Notice and Data Protection Policy (available from NIPSA HQ and on our website).**

I agree to be contacted by NIPSA for this purpose and for NIPSA to hold my personal information as supplied by me/my union for that purpose. I understand that my personal data will be retained for this purpose and will be deleted when the specific activity has ceased/come to an end (i.e. end of term of office of Committee or the end of a campaign etc.).

Name:

Union:

Email:

Phone/Mobile:

Signature:

Appendix 3

DATA SECURITY (RETENTION AND DISPOSAL) POLICY

The following policy outlines how you should use/hold/retain and destroy (when necessary) all personal data that you hold for the *'legitimate purpose'* of carrying out your role, in any capacity, on behalf of NIPSA. It is our duty not only to ensure that we treat our members' data appropriately but that this is informed by our obligations under Regulation (EU) 2016/679 of the European Parliament and the Council commonly referred to as the General Data Protection Regulations (GDPR). In addition to detailed instruction to staff that have been issued re, inter alia, conferences (Main and Group, Health and Safety, Union Learning etc.); the Membership Office; Finance; Personnel etc. please note the following.

PERSONAL CASES

"Personal Case" files **must be destroyed no later than 2 years after the case file is opened unless the case is still live.** With immediate effect you should review all personal case files held in your office and destroy **by confidential means** all files that have been held for longer than 2 years. If you intend to retain any file for more than 2 years you **must** have a legitimate reason for doing so such as *"case ongoing"*. A further review of this file must take place no later than 12 months after this decision to retain. If you wish to keep a file for longer than 2 years and the reason for doing so is not *"case ongoing"* discussion and agreement to do this must take place with your line manager/HQ Official. (See **File Review Form at Appendix 5)** that will assist you in this process.)

Security: Both paper and electronic copies of personal case files/data should be treated the same. Therefore any electronic files (including that on your phone) must comply with our policies/instructions/procedures re use, retention, deletion of personal case files etc. Any file or papers relating to an individual must be kept out of the view of visitors to your office/building with *"current"* files secured during the day when not in use and papers records stored in a **locked** filing cabinet overnight. In terms of other security measures remember to:

- **Lock away laptops when you are not in the office** and ensure all computers and laptops are suitably password protected and/or encrypted.
- **Think about data security if taking files home**: If you take a file home – it must be done with security in mind e.g. in closed bag or sealed envelope. Do not leave documents/laptops etc. in car overnight. If *"data"* is brought into the home it must be kept and stored safely/securely. This is to ensure that in the unlikely event of your home being burgled that all reasonable steps have been taken to ensure a member's data has been held securely.

- Encrypt or password protect documents containing special categories of data such as union membership.

EMAILS

When you send **emails** to members (or non-members) remember that you must not disclose someone's union membership to anyone else. **If you are sending an email to a number of recipients and identifying them as either members or non-members use the *"bcc"* (blind carbon copy) field in the email to list their addresses and send it to yourself.** In this way, yours will be the only email address that is visible.

Appendix 4

DATA PRIVACY IMPACT ASSESSMENT (DPIA*)

What personal data will be collected?	
Why will this personal data be collected?	
Who will it be processed by (and who will have access)?	
Who will it be shared with?	
Where will it be processed and stored?	
When will it no longer be needed?	
How was consent acquired?	
Legal basis for collecting the data?	
Security measures employed to protect data?	
Risks to Individual of breach of privacy?	
Risks to organisation i.e. compliance risks, reputational damage etc.	

Signed:

Date:

*Any data processing carried out on behalf of NIPSA is done on the legal basis outlined in our Privacy Notice and Data Protection Policy (available from NIPSA HQ and on our website). A DPIA must be carried out where there the type of data processing that is being considered carries a "high risk of infringing individuals' rights and freedoms, particularly where it uses new technology." (The General Data

Protection Regulations- A practical guide for trade unionists, March 2018, Labour Research Department).

Should such activity be contemplated, advice must be sought from the Data Protection Officer, NIPSA HQ.

nipsa Personal Case: File Review

Protecting Public Services
Supporting Public Servants

Name:	
Address: (inc Postcode)	
Contact Telephone Number(s):	
NIPSA Membership Number:	
Date file opened:	1st Review Date: (2 years after opening)
Reason for holding for longer than 2 years:	
2nd Review Date:	

nipsa
Protecting Public Services
Supporting Public Servants

028 9066 1831 info@nipsa.org.uk www.nipsa.org.uk

Headquarters
54 Wellington Park, Belfast, BT9 6DP
Tel: 028 9066 1831

Regional Office
30 Great James Street, Derry, BT48 7DB
Tel: 028 7137 4977

40107