Nexus

Data Protection Policy and Procedures

This document includes a policy statement and guidance on Data Protection as it affects Nexus. It is recognised that this is a broad and complex topic and the guidance is, for clarity and simplicity of content, confined to those aspects of personal data protection which are most prevalent in core day to day activities within Nexus.

Personal data is any information which the Group holds and or uses on individuals.

Where an 'individual' is defined as;

- An employee (existing, past or prospective or agency staff);
- A customer or prospective customer; sub-contractors and suppliers.

The law equally applies to personal data whether it is held on electronic or paper media. A full set of definitions is included at appendix A.

1. Policy

Nexus are aware of the need to meet the legal requirements concerning protection of personal data particularly as invoked in the Data Protection Act 1998 and the Privacy and Electronic Communications Regulations 2003 and enforced in the UK by the Office of the Information Commissioner (OIC).

Nexus tries to ensure a 'culture in which respect for private life, data protection, security, and confidentiality of personal information is seen as the norm'. Methods of ensuring that the legal requirements are met have been established for Nexus and are subject to routine monitoring and auditing.

The Eight Data Protection Principles

- Personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless:
- At least one of the conditions set out in appendix B are met.
- In the case of sensitive personal data, at least one of a further set of conditions set out in appendix C is met.

- Personal data shall be obtained for only one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose.
- Personal data shall be adequate, relevant and not excessive in relation to the purpose for which they are processed.
- Personal data shall be accurate and, where necessary, kept up to date.
- Personal data processed for any purpose shall not be kept for longer than is necessary for that purpose.
- Personal data shall be processed in accordance with the rights of data subjects under the Act.
- Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.
- Personal data shall not be transferred to a country or territory outside the European Economic Areas unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

Nexus aspire to the data security requirements as set out in ISO 27001.

2. Responsibilities

The Managing Director is the central point of contact for all data protection issues. The MD ensures company policy and practice are incompliance with the eight data protection principles.

3. Guidance

There follows guidance which discusses both general and discipline specific issues related to personal data protection. This guidance seeks to customise and simplify the key data protection requirements relative to the Nexus. This guidance is by no means exhaustive and will be subject to review and amendment through time. For clarity the guidance is in two parts related firstly to clients subcontractors and partners organisations and then to employees (existing, past). Due to its fundamental importance in processing data a specific list of additional guidance related to IT is also included.

In order to allow an overview of successful implementation the various disciplines will be subject to routine audit to ensure compliance with the legal requirement.

3.1 Related to clients, subcontractors, and partner organisations

1) Personal Data gathered from customers, subcontractors, and partner organisations should be for a specific purpose which is made known to the individual and should not be used for any other purpose unless as outlined below. (Typically an application for a particular product) A list of acceptable reasons for processing personal data is given in appendix B.

2) The minimal personal data required to allow the required process should be recorded.

3) If the data is intended for any other purpose then, as a minimum, a standard opt-out clause should be included in the agreement. This agreement can in some instances be

verbal (e.g. taken over the phone - but the resultant decision should be recorded) (see appendix D)

4) Where the data could be used for electronic marketing communications an opt-in agreement is required (see appendix D).

5) All forms of direct marketing will use data which has been subject to data protection permissions unless the individual is aware that the data was gathered specifically for direct marketing purposes. (see appendix D).

6) Email rental lists shall not be used by marketing unless data protection permissions can be demonstrated to have been given.

7) Departments should in general not hold sensitive personal data about an individual (see appendix C) (Such data should not be required of clients and generally for employees should be held by HR).

8) All data held on individuals should be accurate and up to date.

9) Data should only be sent outside of the Nexus (e.g. to a printing company) where the requirements in appendix E are met.

10) The Nexus remain responsible for data sent to partners, subcontractors and suppliers and must take adequate steps to ensure that the data is only used in accordance with instructions.

11) Data must be protected against unauthorised processing, damage, accidental loss or destruction.

12) Data should not be sent outside the European Economic Area unless the conditions in appendix H are met.

13) Data should not be retained for a greater period than necessary for the purpose for which it was acquired (see appendix H).

14) Upon request the group must disclose any personal data it holds on an individual. This is called a data disclosure request.

15) Data shall be held in a manner which allows a customers data disclosure request for all permanent form data relating to them to be supplied within 40 days. (Exemptions to this requirement are listed in appendix E).

16) Records of such data disclosure requests and responses shall be maintained.

17) Where a data subject requests that evaluation decisions concerning them should not be by electronic means alone then alternatives will be established (For example if we were to electronically score and prioritise suppliers)

3.**2 Related to Employees (existing, past prospective or agency)**

Data held on employees shall be the minimal required for the specific purposes related to employment and shall not be used for any other purpose without the positive consent of the employee. A list of acceptable reasons for processing personal data is given in appendix B.

Training on data protection related both to employee data and client data shall be included in induction training. Wherever practicable only HR should have access to sensitive personal data concerning employees (see appendix D).

4) Conditions for the lawful processing of sensitive personal data are set out in appendix C.

5) All data held on individuals should be accurate and current.

6) Data on employees can only be sent outside of Nexus where the conditions in appendix F are met.

7) Data should not be sent outside the European Union unless the conditions in appendix G are met.

8) Nexus remain responsible for data sent outside of the group and must take adequate steps to ensure that the data is only used in accordance with instructions.

9) Data must be protected against unauthorised processing, damage, accidental loss or destruction.

10) Data should not be retained for a greater period than necessary for the purpose for which it was acquired (see appendix H).

11) Data shall be held in a manner which allows an employee access to data held about them upon request. Note that where data also relates to other employees then this need not necessarily be included. (Exceptions to this requirement are listed in appendix E).

12) Records of such data disclosure requests and responses shall be maintained.

13) Where a data subject requests that evaluation decisions concerning them should not be by electronic means alone then alternatives must be established. (e.g. electronic scoring of employees performance).

14) The business makes use of CCTV for reasons of security and occasionally to provide data on events such as incidents in the car parking area. Access to this data is strictly limited to those who need to know and no personal data will be disclosed other than for the business purposes described.

4. IT (Areas specific to IT and stressing some issues raised earlier)

Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.

Consideration should be given to technical security arrangements, both internal and external, including password protection, virus protection software, firewalls, data encryption, and building security measures.

Security must be borne in mind also where personal data is being destroyed.

IT should aspire to the data security requirements as set out in ISO 27001.

Where personal data is to be carried out by a data processor (mailing houses, printing companies etc.) on behalf of the organisation the selection criteria must include guarantees in respect of the technical and organisational measures governing the processes to be carried out (see appendix F).

Data must be protected against unauthorised processing, damage, accidental loss or destruction.

Data should not be retained for a greater period than necessary for the purpose for which it was acquired (see appendix H).

8) Data shall be held in a manner which allows data disclosure request for all permanent form data relating to them to be supplied within 40 days

(Exemptions to this requirement are listed in appendix E).

9) Records of such data disclosure requests and responses shall be maintained.

Appendix A

Definitions

1. Data Subject

An individual who is the subject of personal data including:

• Employees

• Past employees

• Prospective employees

• Customers

• Partners

• Prospective customers

• Agency staff

• Subcontractors

• Suppliers

2. Personal Data

Any information that an organisation holds and/or uses on individuals, including:

a) Employees

• Name and address

• Age and date of birth

• Telephone number

• Salary details and bank account information

• Next of kin details

• Appraisal disciplinary and holiday records

• Sickness and medical records

• Previous work history

b) Clients, subcontractors and suppliers

• Name of company and address

• Application data

• Visit reports

• Submitted information such as training or registration certificates

• Bank account details

• Telephone number

2. Data Controller

The organisation that determines how personal data will be used.

3. Data Processor

An organisation that processes personal data on behalf of a Data Controller, e.g.

• Mailing Houses

• Printing Companies

Appendix B

Reasons for using Personal Data

Personal data shall not be processed unless one of the following legitimising conditions applies.

1. The data subject has given consent to the processing.

2. The processing is necessary;

- for the performance of a contract to which the data subject is a party.
- for the taking of steps at the request of the data subject with a view to entering into a contract.

3. The processing is necessary for compliance with any legal obligation to which the data controller is subject, other than an obligation imposed by contract.

4. The processing is necessary in order to protect the vital interests of the data subject.

5. The processing is necessary:

- for the administration of justice.
- for the exercise of any functions conferred on any person by or under any enactment.
- for the exercise of any functions of the Crown, a Minister of the Crown or a government department.

for the exercise of any other functions of a public nature exercised in the public interest by any person.

the processing is necessary for the purposes of legitimate interests pursued by the data controller or by the third party or parties to whom the data are disclosed, except where the processing is unwarranted in any particular case by reason of prejudice to the rights and freedoms or legitimate interests of the data subject.

Appendix C

Sensitive Personal Data and The reasons for using Sensitive Personal Data

Sensitive personal Data is:

a) The racial or ethnic origin of the data subject.

b) The subjects political opinions.

c) Religious beliefs or other beliefs of a similar nature.

d) Membership of a trade union.

e) Physical or mental health.

f) Sexual life.

g) Criminal activity.

The nineteen reasons for the lawful processing of sensitive personal data one of which must be met are as follows:

1) Explicit consent of the data subject.

2) Compliance with employment law obligations.

3) Vital interests of the data subject.

4) Processing by not for profit organisations.

5) Information made public by the data subject.

6) Legal advice and establishing of defending legal rights.

7) Public functions (administration of justice. Etc.)

8) Medical purposes.

9) Records on racial equality.

10) Detection of unlawful activity.

11) Protection of the public.

12) Public interest disclosure.

13) Confidential counselling.

14) Certain data relating to pensions.

15) Religious and health data for equality of treatment monitoring.

16) Legitimate political activities.

17) Research activities that are in the substantial public interest.

18) Police processing.

19) Processing by elected representatives.

Appendix D

Opt Out and Opt in for Customer Personal Data

Where customers and partners personal data may be used for a purpose other that that for which the data was obtained then permission for that use must be obtained typically by use of an opt out or opt in clause. Where the data will be processed electronically to allow it to be used for other purposes then an opt in permission is required.

Examples of opt out and opt in clauses are as follows:

Example 1: Opt Out

The Nexus would like to keep you informed of other activities carried out by the organisation which may be of interest to you. Please tick this box if you do not wish us tokeep you informed.

Example 2: Opt In

Please tick this box if you would like Nexus to keep you informed of other activities carried out by the group which may be of interest to you.

Appendix E

Exemptions to Right of Subject Access

The right of subject access is extremely wide ranging and unless a relevant exemption applies (see below) an individual is generally entitled to see their personal data.

Exemptions

- Management forecasting – personal data used for this purpose is exempt from disclosure for as long as the management forecasting activity continues.

- Negotiations – personal data used for this purpose is exempt from disclosure for as long as the negotiations continue.
- Disproportionate effort – Rarely, it may be possible for a data controller to show that the effort that it would take to retrieve the requested information is too great.
- Confidential references – the author of a confidential reference is exempt from the need to disclose that reference.
- Prevention / detection of crime.
- Material disclosing third party information.
- Legal professional privilege (e.g. communication with the organisation's lawyers concerning an employee.

Appendix F

Using third parties to process data

Where data is sent outside the group to be processed then responsibility for that data remains with Nexus and safeguards to ensure its protection must be taken including:

- Ensuring that the third party provides sufficient guarantees in respect of the technical and organisational security measures governing the process being carried out (typically by agreeing a contract which includes contractual requirements on data protection).
- Taking reasonable steps to ensure compliance with these measures (This can be limited to the above for simple processes but could extend to visits to the third parties premises where greater control is appropriate) Examples of third parties are call centres, printers, mailing houses, website hosts, etc.

Considerations in contracts and controls applicable to third parties should include:

- Ensure that the processing by the third party is only in accordance with the Nexus's instructions.
- Ensure that the processing is undertaken only for the purposes and in the manner stated in the contract.
- Ensure the third parties staff are trained in data security measures.
- Ensure that there is a contractual undertaking in place which includes requirements to implement personal data security measures.
- Ensure that where appropriate the group has the right of access to the third party premises to ensure the security measures are being implemented.
- Restrict the third parties ability to sub-contract the process and its obligations.

Appendix G

Sending Data Abroad

'Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.'

The EEA countries are as follows:

Austria; Belgium; Bulgaria; Cyprus; Czech Republic; Denmark; Estonia ; Finland; France; Germany; Greece; Hungary; Iceland; Ireland; Italy; Latvia; Lichtenstein; Lithuania; Luxemburg; Malta; Netherlands; Norway; Poland; Portugal; Romania; Slovak Republic; Slovenia; Spain; Sweden; United Kingdom.

There are various exemptions (derogations) called out in schedule 4 of The Data

Protection Act 1998.

The principal derogation which will be of interest to the group is:

1. The data subject has given his consent to the transfer.

2. The transfer is necessary:

a) For the purpose of a contract between the data subject and the data controller.

b) For the taking of steps at the request of the data subject with a view to his entering into a contract with the data controller.

3. The transfer is necessary:

a) For the conclusion of a contract between the data controller and a person other than the data subject which is entered into at the request of the data subject or is in the interests of the data subject.

b) For the performance of such a contract.

4. The transfer:

a) Is necessary for the purpose of, or in connection with, any legal proceedings.

b) Is necessary for the purpose of obtaining legal advice,

c) Is otherwise necessary for the purposes of establishing, exercising; or defending legal rights. It is strongly recommended that where data is transferred outside the EEA that the

Managing Director is consulted to allow the process to be legally compliant.

Appendix H

Data Retention Times Recommendations

Accounting Records: As required by HMIT and customs and excise (usually 6

years).

Employee Records: Tax records for 6 years, Personnel records for 3 years after data subject leaves then a summary record for a further 3 years.

General Correspondence: Current and Previous year.

Authorised by

Bob Woods
Managing Director
Nexus National Security Network
Prestige Court
Beza Road
Leeds LS10 2 BD
Bob.Woods@NexusNSN.co.uk
T: 0845 680 5726

A full copy of this statement is available upon request.