PART OF nocn GROUP

Data Protection (EPA)

Data Protection

1. Introduction

NOCN Group refers to NOCN and all subsidiaries for example One Awards, Job Cards and any future subsidiaries.

In order to operate efficiently and effectively, NOCN Group must collect personal data about individuals it works with and colleagues. This may include learners, suppliers, individuals with an NOCN Job Card, employees (past, current and prospective), casual workers, sub-contractors, Centre representatives, Board and Committee members, and others with whom it communicates.

NOCN Group are also required to collect and use information in order to comply with regulatory and statutory requirements.

The processing of personal data must be dealt with in accordance with the regulations as stated under the Data Protection legislation to ensure compliance. The legislation regulates the way the personal data collected is handled and gives certain rights to individuals relating to their personal data. See Appendix One for the Information Commissioner's Office (ICO) guidance on 'Who does the Data Protection Legislation apply to?'

NOCN Group considers that the correct processing of personal data is integral to the success of its operations and to maintaining the trust of the individuals it deals with. The underlying principles of the legislation are fundamental to NOCN Group operations and it fully supports and adheres to its provisions. Appendix Two lists the principles of the current legislation in full, and they can be summarised as follows.

Data must be:

1. Fairly and lawfully processed
2. Processed for limited purposes
3. Adequate, relevant and not excessive
4. Accurate
5. Not kept longer than necessary
6. Secure

NOCN Group and its subsidiaries are Data Controller's and are registered with the Information Commissioner to process personal data. Each subsidiary of NOCN Group will have its own registered Data Protection Officer for clarification on who holds this position at each subsidiary please see contact details at the end of this document. A structure detailing the various roles and who to contact regarding different data areas is attached see Appendix Seven.

The legislation requires that the Data Controller shall be responsible for, and be able to demonstrate, compliance with the principles outlined above.

NOCN Group shall not sell, rent, distribute or otherwise make user data commercially available to any third party, except as described above, or with prior consent.

The security of the data NOCN Group holds is a key priority and in order to ensure that the IT systems are safe and secure it has vigorous procedures in place which are regularly reviewed.

2. Data covered by the Data Protection Legislation

The legislation uses the term “personal data”. Regarding data we hold, personal data essentially means any recorded data held by NOCN Group (either electronically or in paper format) from which a living individual can be identified either directly or indirectly. This may include a variety of data including names, addresses, telephone numbers, unique identity numbers, photographs of individuals, online identifier and other personal details.

Appendix Three details the ICO definition on processing and ‘What data does the Data Protection Legislation apply to?’.

3. Right of Access

Individuals have the right to obtain their personal data from us. If any individual wishes to exercise the right to access their personal data, they should make the request in writing to NOCN Group, please see attached structure at Appendix Seven. There is no fee applied to a data access request, but a charge may be applied if the request is considered excessive or for multiple copies. The fee would always be communicated in advance of processing and approval sort to continue with the request.

The data will be provided within 28 calendar days. It can be extended by a further two months where requests are complex or numerous, although NOCN Group will inform the individual of the delay and the explanation, within 28 days of receipt of the request.

The legislation provides the following rights for individuals:

- The right to be informed
- The right of access
- The right to rectification
- The right to erasure
- The right to restrict processing
- The right to data portability
- The right to object
- Rights in relation to automated decision making and profiling.

Further details relating to the above can be found in Appendix Four ‘Individual rights.

4. Lawful Basis for processing

In order to process personal data NOCN Group must have a valid lawful basis under Article 5. The lawful basis will depend on the purpose of the data and the relationship with the individual. It must be determined before the data is processed and should be documented and stated within the privacy notice.

The six type of lawful basis are:

- Consent – individual has given clear consent for a specific purpose
- Contract – necessary for a contract or specific step prior to a contract
- Legal Obligation – necessary to comply with the law
- Vital interests – necessary to protect someone’s life
- Public task – necessary to perform a task in the public interest with a clear basis in law
- Legitimate interests – necessary for the organisations or a third party’s legitimate interest

Further details relating to the six types of lawful basis can be found in Appendix Five.

If NOCN Group processes data classed as special category data an additional lawful basis will be required, documented and again included within the privacy notice. See Appendix Six for further details.

The processing of criminal conviction data or data about offences is classed separately and will require a lawful basis under Article 6 and either legal or official authority under Article 10. See Appendix Six for further details.

5. Accountability and Governance

Accountability and governance are significant within the current Data Protection legislation. Privacy impact assessments and privacy by design are now legally required in certain circumstances. These measures should minimise the risk of breaches and uphold the protection of personal data. NOCN Group takes protecting data seriously and ensures that all measures are in place.

NOCN Group will ensure that it is compliant by:

- implementing appropriate technical and organisational measures. This may include internal data protection policies such as staff training, internal audits of processing activities, and reviews of internal HR policies
- maintain relevant documentation on processing activities
- appoint a Data Protection Manager and a working group
- implement measures that meet the principles of data protection by design and data protection by default.

Measures could include:

- data minimisation (only collect relevant data and retain as long as necessary)
- pseudonymisation (process the data in such a way to render it anonymous)
- transparency
- allowing individuals to monitor processing
- creating and improving security features on an ongoing basis
- use data protection impact assessments (DPIA) where appropriate.

The necessity for a DPIA will be considered as part of the initial development of each project relating to data processing.

The Board of Trustees will monitor the compliance of Data Protection Legislation by reviewing the annual report submitted by the Data Protection Officer. The annual report will include assurances on the level at which NOCN Group is operating within the legislation including an overview of the external facing documents being fit for purpose. It will also report on any data incidents occurring during that time period although, if a serious breach occurs they will be informed immediately as stated within the Data Breach Policy.

6. Contracts

NOCN Group will ensure that any data processor (a third party who processes personal data on behalf of the controller) will have a written contract in place detailing their obligations, responsibilities and liabilities as detailed within the Data Protection legislation. Only processers who can provide sufficient guarantees that they comply with the legislation will be appointed by NOCN Group.

7. Personal Data Breaches

The legislation introduces a duty to all organisations to report certain types of personal data breach to the relevant supervisory authority, within 72 hours of becoming aware of the breach, where feasible. In the case of a breach where it is likely to result in a high risk of adversely affecting individuals' rights and freedoms, NOCN Group will inform those individuals without undue delay. NOCN Group has robust breach detection, investigation and internal reporting procedures in place which will facilitate decision-making about whether to notify the relevant supervisory authority and the affected individuals. A record of any personal data breaches will be maintained detailing the facts relating to the breach, its effects and the remedial action taken.

Personal data breaches can include:

- access by an unauthorised third party
- deliberate or accidental action (or inaction) by a controller or processor
- sending personal data to an incorrect recipient
- computing devices containing personal data being lost or stolen
- alteration of personal data without permission, and
- loss of availability of personal data.

A personal data breach can be broadly defined as a security incident that has affected the confidentiality, integrity or availability of personal data. In short, there will be a personal data breach whenever any personal data is lost, destroyed, corrupted or disclosed if someone accesses the data or passes it on without proper authorisation or if the data is made unavailable and this unavailability has a significant negative effect on individuals.

8. Our Commitment to Data Protection

We will ensure that:

- everyone managing and handling personal information understands that they are responsible for following good data protection practice
- there is someone with specific responsibility for data protection in the organisation
- staff who handle personal information are appropriately supervised and trained
- queries about handling personal information are promptly and courteously dealt with, and individuals know how to access their own personal information
- methods of handling personal information are regularly assessed and evaluated
- any disclosure of personal data will be in compliance with approved procedures
- all necessary steps are taken to ensure that personal data is kept secure
- all software updates have been installed on all Servers and Computers and that a regular schedule of maintenance is carried out
- where necessary and required by regulation, such as data provided by the Education and Skills Funding Agency, access to this data will be restricted by folder to those approved access by the Third Party
- NOCN Group will comply with all time scales for Data Retention, as stipulated in the NOCN Group Retention Policy. Where data has been provided by a Third Party, such as the Education and Skills Funding Agency, the Data will only be retained for as long as stipulated in any Data Sharing Agreement, where there is no retention period stipulated, the NOCN Group Data Retention Policy will be implemented.

Further Information

Further information on the application of this Policy and practice may be obtained from Dawn Rush, or from the Information Commissioner's Office: http://www.ico.org.uk/

Contact Details
NOCN Group
Acero Building
1 Concourse Way
Sheaf Street
Sheffield
S1 2BJ

Telephone Number: 0300 999 1177

Email Address: Simon.renny@nocn.org.uk or dataprotection@nocn.org.uk

Website: www.nocn.org.uk

Appendix One:

Who does the Data Protection Legislation apply to?

- the Data Protection Legislation applies to 'controllers' and 'processors'
- a controller determines the purposes and means of processing personal data
- a processor (third party) is responsible for processing personal data on behalf of a controller
- a processor under the Data Protection Legislation has specific legal obligations. Processors are required to maintain records of personal data and processing activities and are legally liable if responsible for a breach
- controller is not relieved of any obligations where a processor is involved – the Data Protection Legislation places further obligations to ensure that contracts with processors comply with the Data Protection Legislation
- the Data Protection Legislation applies to processing carried out by organisations operating within the UK. It also applies to organisations outside the UK that offer goods or services to individuals in the UK
- GDPR applies to organisations which process data within the EU
- the Data Protection Legislation does not apply to certain activities including processing covered by the Law Enforcement Directive, processing for national security purposes and processing carried out by individuals purely for personal/household activities.

Appendix Two:

Article 5 of the Data Protection Legislation requires that personal data shall be:

- processed lawfully, fairly and in a transparent manner in relation to individuals
- collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes

- adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed
- accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay
- kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the Data Protection Legislation in order to safeguard the rights and freedoms of individuals, 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.

Appendix Three:

What data does the Data Protection Legislation apply to?

Personal data

The Data Protection Legislation applies to 'personal data' meaning any information relating to an identifiable individual who can be directly or indirectly identified in particular by reference to an identifier.

This definition provides for a wide range of personal identifiers to constitute personal data, including name, identification number, location data or online identifier, reflecting changes in technology and the way organisations collect information about individuals.

The Data Protection Legislation applies to both automated personal data and to manual filing systems where personal data are accessible according to specific criteria.

Personal data that has been pseudonymised can fall within the scope of the Data Protection Legislation depending on how difficult it is to attribute the pseudonym to a particular individual.

Sensitive personal data

The Data Protection Legislation refers to sensitive personal data as "special categories of personal data''. This is because special category data is more sensitive, and so needs more protection.

For example, information about an individual's:

- race
- ethnic origin
- politics
- religion
- trade union membership
- genetics
- biometrics (where used for ID purposes)
- health
- sex life or
- sexual orientation.

The special categories specifically include genetic data, and biometric data where processed to uniquely identify an individual. In particular, this type of data could create more significant risks to an individual's fundamental rights and freedoms.

Criminal offence data

Personal data relating to criminal convictions and offences are not included and are dealt with separately but similar extra safeguards apply to its processing (see Article 10 for further details).

Processing

Processing means 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.

Appendix Four:

Individual rights

A copy of the data held must be made available free of charge. A 'reasonable fee' can be charged, or a request refused when it is considered to be manifestly unfounded or excessive, particularly if it is repetitive.

The fee must be based on the administrative cost of providing the information. Data must be provided without delay and at the latest within 28 days of receipt.

It can be extended by a further two months where requests are complex or numerous, although the individual must be informed of the delay and the explanation, within one month of receipt of the request.

If a request is refused, it must be explained why to the individual, informing them of their right to complain to the supervisory authority and to a judicial remedy without undue delay and at the latest within one month.

The identity of the individual making the request should be verified using reasonable means. If the request is made electronically, then the information should be provided in a commonly used electronic format. Where you process a large quantity of information about an individual, the Data Protection Legislation permits you to ask the individual to specify the information the request relates to.

Rights to be informed

The individual's right to be informed encompasses the requirement to provide 'fair processing of data' with an emphasis in transparency on how the personal data is used.

The information on the processing of personal data must be:

- Concise, transparent, intelligible and easily accessible
- Written in clear and plain language
- Free of charge.

The information supplied is determined by whether or not the personal data was obtained direct from individuals. See the table below for further information on this.

What should be supplied	Data direct from data subject	Data indirectly obtained
Data Controller and data protection officer details	Yes	Yes
Purpose of the processing and the lawful basis	Yes	Yes
Legitimate interests of the controller or third party	Yes	Yes
Categories of personal data		Yes
Recipient of the personal data	Yes	Yes
Details of transfers to third country and safeguards	Yes	Yes
Retention period	Yes	Yes
Data subject rights	Yes	Yes
Right to withdraw consent if applicable	Yes	Yes
Right to complain with a supervisory authority	Yes	Yes
Source of the personal data		Yes
Details of consequences of not providing if personal data is statutory or contractual	Yes	
Details of automated decision making	Yes	Yes
When the information should be provided	At the time obtained	Within a reasonable period (within one month)

Right of access

Individuals have the right to access their personal data and supplementary information. It allows individuals to be aware of and verify the lawfulness of the processing.

Best practice recommendation in Data Protection Legislation states that, where possible, organisations should be able to provide remote access to a secure self-service system which would provide the individual with direct access to his or her information (Recital 63). The right to obtain a copy of information or to access personal data through a remotely accessed secure system should not adversely affect the rights and freedoms of others.

Right to rectification

The Data Protection Legislation gives individuals the right to have personal data rectified if it is inaccurate or incomplete.

If personal data in question has been disclosed to others, each recipient must be informed of the rectification - unless this proves impossible or involves disproportionate effort. If asked the individual must be informed of the recipients.

Right to erasure/or to be forgotten

The broad principle underpinning this right is to enable an individual to request the deletion or removal of personal data where there is no compelling reason for its continued processing.

The right to erasure does not provide an absolute ‘right to be forgotten’. Individuals have a right to have personal data erased and to prevent processing in specific circumstances:

- where the personal data is no longer necessary in relation to the purpose for which it was originally collected/processed
- when the individual withdraws consent
- when the individual objects to the processing and there is no overriding legitimate interest for continuing the processing

- the personal data was unlawfully processed (i.e. otherwise in breach of the Data Protection Legislation)
- the personal data has to be erased in order to comply with a legal obligation
- the personal data is processed in relation to the offer of information society services to a child.

Under the Data Protection Legislation, this right is not limited to processing that causes unwarranted and substantial damage or distress. However, if the processing does cause damage or distress, this is likely to make the case for erasure stronger.

There are some specific circumstances where the right to erasure does not apply and a request can be refused when:

- to exercise the right of freedom of expression and information
- to comply with a legal obligation for the performance of a public interest task or exercise of official authority
- for public health purposes in the public interest
- archiving purposes in the public interest, scientific research historical research or statistical purposes or
- the exercise or defence of legal claims.

There are extra requirements when the request for erasure relates to children's personal data, reflecting the Data Protection Legislation emphasis on the enhanced protection of such information, especially in online environments.

If personal data of children is processed, special attention must be considered to existing situations where a child has given consent to processing and they later request erasure of the data (regardless of age at the time of the request), especially on social networking sites and internet forums. This is because a child may not have been fully aware of the risks involved in the processing at the time of consent (Recital 65).

If the personal data in question has been disclosed to others, each recipient must be contented and informed of the erasure of the personal data - unless this proves impossible or involves disproportionate effort. If asked the individual must be informed of the recipients.

The Data Protection Legislation reinforces the right to erasure by clarifying that organisations in the online environment who make personal data public should inform other organisations who process the personal data to erase links to, copies or replication of the personal data in question.

There may be instances where organisations that process the personal data may not be required to comply with this provision because an exemption applies, see example below.

Example

A search engine notifies a media publisher that it is delisting search results linking to a news report as a result of a request for erasure from an individual. If the publication of the article is protected by the freedom of expression exemption, then the publisher is not required to erase the article.

Right to restrict processing

Individuals have a right to 'block' or suppress processing of personal data, the data can be stored but not processed further.

Restriction to the processing of personal data will be required in the following circumstances:

- Where an individual contests the accuracy of the personal data, processing should be restricted until the accuracy of the data has been verified
- Where an individual has objected to the processing (where it was necessary for the performance of a public interest task or purpose of legitimate interests), and consideration is given to whether the organisation's legitimate grounds override those of the individual.
- When processing is unlawful, and the individual opposes erasure and requests restriction instead
- If the personal data is no longer needed but the individual requires the data to establish, exercise or defend a legal claim.

Procedures may need to be reviewed to ensure that the requirement to restrict the processing of personal data is identifiable.

If the personal data in question has been disclosed to others, each recipient must be contacted and informed of the restriction on the processing of the personal data - unless this proves impossible or involves disproportionate effort. If asked to, the individual must be informed of the recipients.

Individuals must be informed if a decision is made to lift a restriction on processing.

Right to data portability

The right to data portability allows individuals to obtain and reuse their personal data for their own purposes across different services.

It allows personal data to be moved, copied or transferred easily from one IT environment to another in a safe and secure way, without hindrance to usability.

The right to data portability only applies:

- to personal data an individual has provided to a controller
- where the processing is based on the individual's consent or for the performance of a contract and
- when processing is carried out by automated means.

The personal data must be provided in a structured, commonly used and machine-readable form. Open formats include CSV files. Machine readable means that the information is structured so that software can extract specific elements of the data. This enables other organisations to use the data.

The information must be provided free of charge.

If requested the data can be transmitted directly to another organisation if this is technically feasible.

If the personal data concerns more than one individual consideration must be given to whether providing the information would prejudice the rights of any other individual.

Right to object

Individuals have the right to object to:

- processing based on legitimate interests or the performance of a task in the public interest/exercise of official authority (including profiling)
- direct marketing (including profiling) and
- processing for purposes of scientific/historical research and statistics.

Individuals must have an objection on 'grounds' relating to his or her particular situation".

Processing of the personal data must be stopped unless:

- there are compelling legitimate grounds for the processing, which override the interests, rights and freedoms of the individual or
- the processing is for the establishment, exercise or defence of legal claims.

Individuals must be informed of their right to object "at the point of first communication" and in the privacy notice.

This must be 'explicitly brought to the attention of the data subject and shall be presented clearly and separately from any other information'.

A request to stop processing personal data for direct marketing purposes must be stopped as soon as it is received. There are no exemptions or grounds to refuse and must be dealt with at any time and free of charge.

Individuals must have 'grounds relating to his or her particular situation' in order to exercise their right to object to processing for research purposes.

If you are conducting research where the processing of personal data is necessary for the performance of a public interest task, you are not required to comply with an objection to the processing.

If the personal data is necessary for research in the performance of a public interest task, there is no requirement to comply with an objection to the processing.

Rights related to automated decision-making including profiling

The Data Protection Legislation has provisions on:

- automated individual decision-making (making a decision solely by automated means without any human involvement) and
- profiling (automated processing of personal data to evaluate certain things about an individual). Profiling can be part of an automated decision-making process.
- Article 22 of the Data Protection Legislation has additional rules to protect individuals if you are carrying out solely automated decision-making that has legal or similarly significant effects on them.
- you can only carry out this type of decision-making where the decision is:
    - necessary for the entry into or performance of a contract or
    - authorised by Union or Member state law applicable to the controller or
    - based on the individual's explicit consent.
- you must identify whether any of your processing falls under Article 22 and, if so, make sure that you:
    - give individuals information about the processing
    - introduce simple ways for them to request human intervention or challenge a decision
    - carry out regular checks to make sure that your systems are working as intended.

Appendix Five:

Lawful Basis for processing (Article 6)

There are six available lawful basis for processing and each should be applied depending on it being the most appropriate. Under Data Protection Legislation there is an emphasis on accountability and transparency about the choice of the lawful basis. Processing is only lawful if there is a lawful basis under Article 6, and the application of the lawful basis must be demonstrated to comply with the accountability principle in Article 5(2).

The majority of the lawful basis require the processing to be necessary for it to be applied. If the purpose can be reasonably achieved without the processing the basis will not be lawful. Necessary' does not mean that the processing must be essential for the purpose. However, it must be a targeted and proportionate way of achieving that purpose. The lawful basis does not apply if there are other reasonable and less intrusive ways to meet the outcome.

The lawful basis should be determined prior to processing and should be documented with justification of the choice and included within the privacy notice.

Special category data will require an additional lawful basis as will the processing of criminal conviction data or data about offences.

The lawful basis for processing children's personal data requires special consideration.

The lawful basis for your processing can also affect which rights are available to individuals. For example, some rights will not apply:

	Right To Erasure	Right to Portability	Right to Object
Consent			✗[1]
Contract			✗
Legal Obligation	✗	✗	✗
Vital Interest		✗	✗
Public task	✗	✗	
Legitimate Interest		✗	

Consent

Consent is appropriate if individuals have a real choice and control over how their data is used, if this is not the case then consent is not appropriate.

The Data Protection Legislation sets a high standard for consent it is clear that an indication of consent must be unambiguous and involve a clear affirmative action (an opt-in). It specifically bans pre-ticked

[1] but right to withdraw consent

opt-in boxes and also requires individual ('granular') consent options for distinct processing operations.

Consent should be separate from other terms and conditions and should not generally be a precondition of signing up to a service. The consent request should be prominent, concise, separate from other terms and conditions, and easy to understand.

It should include:

- the name of the organisation
- the name of any third-party controllers who will rely on the consent
- what the data is for
- what it will be used for and
- that individuals can withdraw consent at any time

Clear records demonstrating consent must be maintained including who consented, when, how, and what they were told.

There is no set time limit for consent, but it should be regularly reviewed as appropriate.

Explicit consent is similar to the standard consent, but it must be obtained in such a way that there is no room for misinterpretation. The example as stated by the Information Commissioners Office ''the statement should specify the nature of data that's being collected, the details of the automated decision and its effects or the details of the data to be transferred and the risks of the transfer''.

Contract

"Processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract"

The lawful basis for contracts applies when data processing is necessary:

- to fulfil contractual obligations or
- the data subject has requested an action before entering into a contract (e.g. provide a quote).

It does not apply if the contract is with someone different from the individual whose details are being processed.

It does not apply if the pre-contractual steps are at the request of a third party or the organisations initiative.

If processing of special category data is necessary for the contract, a separate condition for processing this data is required. See the guidance on special category data for more information.

If the contract is with a child under 18, consideration should be given as to whether they have the necessary competence to enter into a contract. If there are doubts about their competence, an alternative basis may be considered such as legitimate interests, which can help demonstrate that the child's rights and interests are properly considered and protected. Read the guidance on children and the Data Protection Legislation for more information.
The individual's right to object and the right not to be subject to a decision based solely on automated processing will not apply. However, the individual will have a right to data portability. Read the guidance on individual rights to be informed.

The decision that processing is necessary for the contract must be documented and include information about the purposes and lawful basis in the privacy notice.

Legal Obligation

“Processing is necessary for compliance with a legal obligation to which the controller is subject.”

This lawful basis can be relied on if the personal data is processed to comply with a legal obligation within common law or a statutory obligation. The obligation should be identifiable either by reference to the specific legal provision or to an appropriate source of advice or guidance that sets it out clearly. Regulatory requirements also qualify as a legal obligation for these purposes where there is a statutory basis underpinning the regulatory regime and which requires regulated organisations to comply.

Under the basis of legal obligation, the individual has no right to erasure, right to data portability, or right to object. Read our guidance on individual rights for more information.

Example

The Competition and Markets Authority (CMA) has powers under The Enterprise Act 2002 to make orders to remedy adverse effects on competition, some of which may require the processing of personal data.

A retail energy supplier passes customer data to the Gas and Electricity Markets Authority to comply with the CMA’s Energy Market Investigation (Database) Order 2016. The supplier may rely on legal obligation as the lawful basis for this processing.
A contractual obligation does not comprise a legal obligation in this context. You cannot contract out of the requirement for a lawful basis. However, you can look for a different lawful basis. If the contract is with the individual, you can consider the lawful basis for contracts. For contracts with other parties, you may want to consider legitimate interests.

Vital Interests

“The processing of personal data should also be regarded as lawful where it is necessary to protect an interest which is essential for the life of the data subject or that of another natural individual. Processing of personal data based on the vital interest of another natural individual should in principle take place only where the processing cannot be manifestly based on another legal basis…”

Vital interests can be relied upon as the lawful basis if the processing of the personal data would protect someone’s life. This does not include health data or other special category data if the individual is capable of giving consent, even if they refuse their consent.

Anyone’s vital interests can now provide a basis for processing, not just those of the data subject themselves. For example, if it is necessary to process a parent’s personal data to protect the vital interests of a child.

This lawful basis is very limited in its scope, and generally only applies to matters of life and death. It is likely to be particularly relevant for emergency medical care, when personal data is processed for medical purposes, but the individual is incapable of giving consent to the processing.
In most cases the protection of vital interests is likely to arise in the context of health data. This is one of the special categories of data, which means a condition for processing special category data under Article 9 will need to be identified.

There is a specific condition at Article 9(2)(c) for processing special category data where necessary to

protect someone's vital interests. However, this only applies if the data subject is physically or legally incapable of giving consent. This means explicit consent is more appropriate in many cases, and you cannot in practice rely on vital interests for special category data (including health data) if the data subject refuses consent, unless they are not competent to do so.

Public Task

"Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller"

This lawful basis applies if the personal data is processed:

- in the exercise of official authority'. This covers public functions and powers that are set out in law
- to perform a specific task in the public interest that is set out in law.

When documenting the decision, the relevant task, function or power should be specified, and the statutory or common law basis should be identified.

Any organisation that is exercising official authority or carrying out a specific task in the public interest will rely on this legal basis. The focus is on the nature of the function, not the nature of the organisation.

Individuals' rights to erasure and data portability do not apply if you are processing on the basis of public task. However, individuals do have a right to object. See guidance on individual rights for more information.

Further processing for certain purposes should be considered to be compatible with the original purpose. This means that the original processing of the personal data for a relevant task or function, will be sufficient for any further processing for:

- archiving purposes in the public interest
- scientific research purposes
- statistical purposes.

Legitimate Interests

" Processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child."

Legitimate interest is most likely to be appropriate where data is used in ways that would be reasonably expected and which have a minimal privacy impact, or where there is a compelling justification for the processing.

There are three elements to the legitimate interest's basis (three-part test-Legitimate Interest Assessment), these are:

- Purpose Test: identify a legitimate interest
- Necessity Test: show that the processing is necessary to achieve it and
- Balancing Test: balance it against the individual's interests, rights and freedoms.

The organisation should balance their interests against the individual's. If an individual would not reasonably expect the processing, or if it would cause unjustified harm, their interests are likely to override the organisations legitimate interest.

Legitimate interests as a lawful basis for processing children's data can be considered, but extra care must be taken to ensure their interests are protected. See detailed guidance on children and the Data Protection Legislation.

Legitimate interests can be relied upon to lawfully disclose personal data to a third party although consideration should be given as to why they want the information, whether they actually need it, and what they will do with it. Justification for the disclosure must be demonstrated, but it will be the third party's responsibility to determine their own lawful basis for processing the data.

There is a distinction between one data controller sharing data with another, and a data controller sharing data with its data processor. A data controller using a data processor must have a written contract. A data controller sharing with another data controller does not, but as stated above should consider what the other data controller wants the information, whether they need the information, and what they will do with it.

The Legitimate Interest Assessment should be kept under review if there is a significant change in the purpose, nature or context of the processing.

If the lawful basis for processing is data is legitimate interests, the right to data portability does not apply.

Under legitimate interests for direct marketing, the right to object is absolute and processing must be stopped when someone objects. For other purposes, unless you can show that the legitimate interests are compelling enough to override the individual's rights, processing must be stopped.

Appendix Six:

Special Category Data (Article 9)

Special category data is personal data which is considered more sensitive, and so needs more protection. The list includes the following:

- race
- ethnic origin
- politics
- religion
- trade union membership
- genetics
- biometrics (where used for ID purposes)
- health
- sex life or
- sexual orientation.

In order to lawfully process special category data, there must be a lawful basis for general processing under Article 6 and a separate condition for processing special category data under Article 9. The separate condition should be identified and documented prior to processing special category data.

Special Category Data does not include personal data relating to criminal offences and convictions, as there are separate and specific safeguards for this type of data in Article 10.

In particular, this type of data could create more significant risks to an individual's fundamental rights and freedoms. For example, by putting them at risk of unlawful discrimination.

The conditions are listed in Article 9(2) of the Data Protection Legislation:

- the data subject has given explicit consent to the processing of those personal data for one or more specified purposes, except where Union or Member State law provide that the prohibition referred to in paragraph 1 may not be lifted by the data subject
- processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law in so far as it is authorised by Union or Member State law or a collective agreement pursuant to Member State law providing for appropriate safeguards for the fundamental rights and the interests of the data subject
- processing is necessary to protect the vital interests of the data subject or of another natural individual where the data subject is physically or legally incapable of giving consent
- processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade union aim and on condition that the processing relates solely to the members or to former members of the body or to individuals who have regular contact with it in connection with its purposes and that the personal data are not disclosed outside that body without the consent of the data subjects
- (e) processing relates to personal data which are manifestly made public by the data subject
- processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity
- processing is necessary for reasons of substantial public interest, on the basis of Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject
- processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of Union or Member State law or pursuant to contract with a health professional and subject to the conditions and safeguards referred to in paragraph 3
- processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, on the basis of Union or Member State law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject, in particular professional secrecy
- processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) based on Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.

Criminal offence data (Article 10)

"Processing of personal data relating to criminal convictions and offences or related security measures based on Article 6(1) shall be carried out only under the control of official authority or when the processing is authorised by Union or Member State law providing for appropriate safeguards for the

rights and freedoms of data subjects. Any comprehensive register of criminal convictions shall be kept only under the control of official authority."

To process personal data about criminal convictions or offences, there must be lawful basis under Article 6 and either legal authority or official authority for the processing under Article 10. The data can also be processed if there is official authority and the data is being processed in an official capacity. A comprehensive register of criminal convictions cannot be maintained unless in an official capacity.

The condition for lawful processing of offence data (or identify your official authority for the processing) should be determined and documented before the data is processed.

Appendix Seven:

Definition of roles and responsibilities

Data Controller - a person, company, or other body that determines the purpose and means of personal data processing

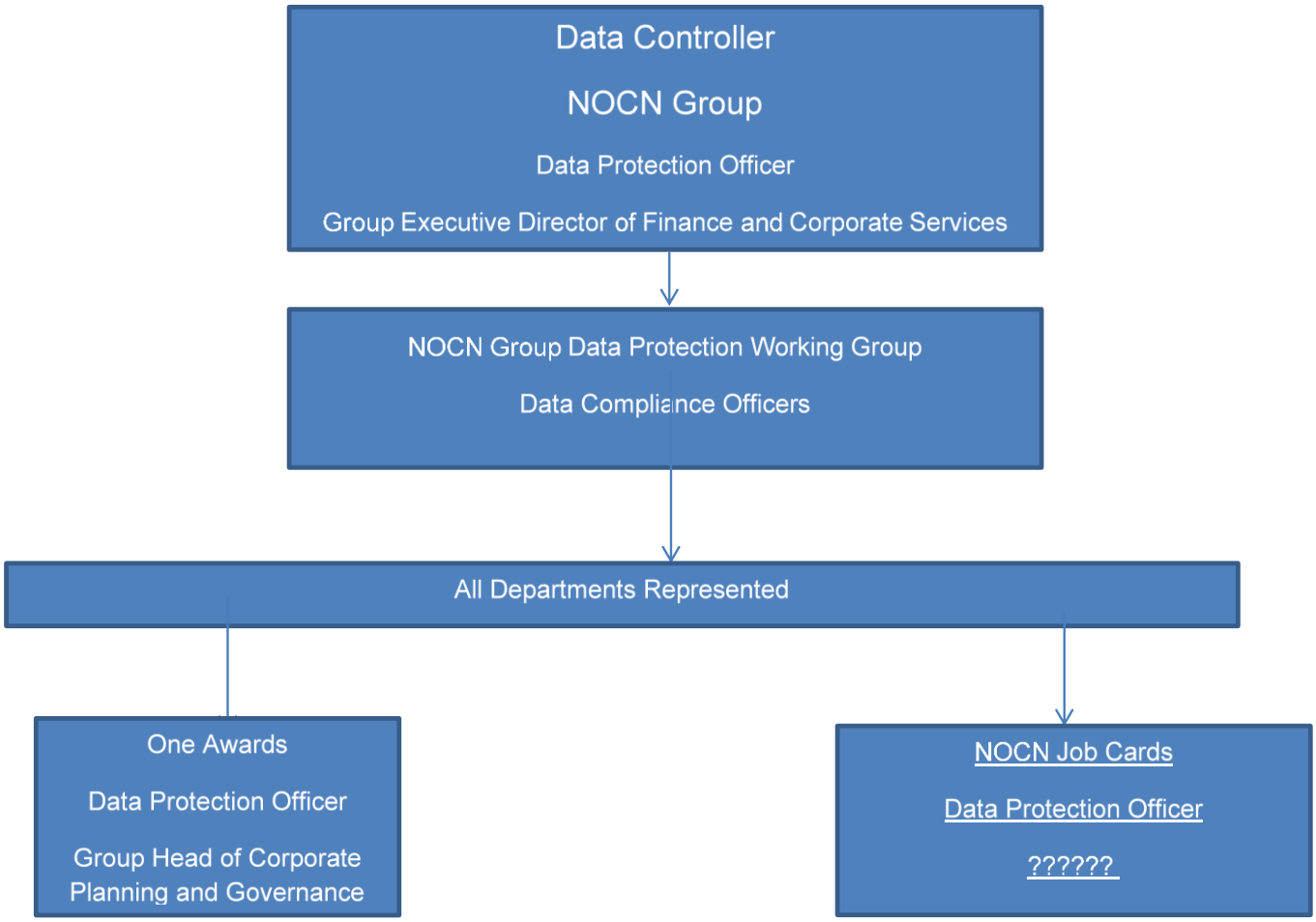
Data Protection Officer/s – report/s directly to the Board and Senior Leadership Team. The role is responsible for internal compliance of data protection obligations and act as a contact point for the supervisory authority.

Data Protection Working Group (DPWG) – is responsible for the operational aspect of implementing the data protection legislation and includes the following:

Review and ensure that policies, procedures and systems comply with all relevant legislation and make recommendations.

- Ensure that all staff, including sub-contractors, access training and updates with regards to data protection to maintain their understanding and knowledge and promote good practice.
- Upskill staff to promote IT and data security across NOCN Group.
- Develop and implement an understanding and awareness of data quality to ensure that staff are aware of the requirements to maintain relevant data.
- Receive and monitor reports from teams across NOCN Group relating to data retention and data cleansing in line with policies.
- Monitor, audit and implement 'tests' to ensure systems are sufficiently robust to meet data protection legislation.
- Act as a source of advice on data protection matters for staff across NOCN Group

Data Compliance Officer - are members of the Data Protection Working Group and represent each of the business units across NOCN. They are responsible for ensuring that the DPWG achieves its objectives.


Data Controller
NOCN Group
Data Protection Officer
Group Executive Director of Finance and Corporate Services
NOCN Group Data Protection Working Group
Data Compliance Officers
All Departments Represented
One Awards
Data Protection Officer
Group Head of Corporate Planning and Governance
NOCN Job Cards
Data Protection Officer
??????

NOCN Group Acero Building 1 Concourse Way Sheaf Street Sheffield S1 2BJ
Tel. 0300 999 1177 Email: endpointassessment@nocn.org.uk Web: www.nocn.org.uk