

Policy Title	Data Protection Policy
Policy Category	Compliant
Owner	Assistant Director Information Governance
Group Executive Lead	Executive Director of Governance, Assurance and Risk
Date Written	February 2019
Considered By	Executive Board
Approved By	Corporation
Date Approved	July 2020
Equality Impact Assessment	The implementation of this policy is not considered to have a negative impact on protected characteristics
Freedom of Information	This document will be publicly available through the Groups Publication Scheme.
Review Date	July 2021
Policy Summary	<p>The aim of this policy is to set standards for processing data and responding to data subject rights requests as required by relevant legislation such as the Data Protection Act 2018 (DPA 2018) and the UK General Data Protection Regulation (GDPR)</p> <p>This policy applies to personal data recorded in any medium, about any person including learners, customers, governors and employees. It also applies to requests made in any format under the rights of the data subject (GDPR Articles 15 to 22).</p>

Applicability of Policy	Consultation Undertaken	Applicable To
Newcastle	Yes	Yes
Newcastle 6th Form	Yes	Yes
Carlisle	Yes	Yes
Kidderminster	Yes	Yes
Lewisham	Yes	Yes
Southwark	Yes	Yes
West Lancashire	Yes	Yes
Professional Services	Yes	Yes

Changes to Earlier Versions	
Previous Approval Date	Summarise Changes Made Here
Feb 2019	Reworking of previous documentation, updating to DPA 2018 compliance.
Feb 2020	Review and minor updates to include references to Governors.
Jul 2020	Annual review – inc confidentiality clauses & simplification.
Jan 2021	Updates to reflect the change in the legislation references after Britain left the European Union.
Linked Documents	
Document Title	Relevance
FOI and EIR Policy	Directly relates to the operation of this document.
Information Policy	Directly relates to the operation of this document.
NCG Special Category Data and Criminal Convictions Data Policy	Directly relates to the operation of this document.

## NCG Data Protection Procedures

### 1. Definitions

Data Protection Legislation	Data Protection Act 2018 (DPA 2018) United Kingdom General Data Protection Regulation (GDPR)
Data Subject	Means people to whom data relates: all prospective, current and previous employees, learners, customers sub-contractors, partners, suppliers, contacts, governors, referees, friends or family members of employees and learners.
Data Controller	Means 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.
Data Processor	Means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.
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.
Personal Data	Any information in relation to an identified or identifiable living individual. "Identifiable living individual" means a living individual who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data or an online identifier, or one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of the individual.
Special Categories of 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 natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.
Criminal Convictions and Offences Data	Personal data relating to criminal convictions and offences under Article 10 (GDPR)
Employees	All current, previous and prospective members of staff.
Learners	All current, previous and prospective customers, clients, participants or programme participants.
Official Information	Information that relates to the organisation and its activities.
Supervisory Authority	The independent public authority responsible for data protection. The supervisory authority for NCG is the Information Commissioner's Office (ICO)
Privacy and Electronic Communications Regulations (PECR)	The Privacy and Electronic Communications (EC Directive) Regulations 2003.

### 2. Introduction

These procedures:

- Are designed to ensure compliance with the Data Protection Act 2018, the United Kingdom General Data Protection Regulation (GDPR) & the Common Law Duty of Confidence.
- Apply to all managers, staff, learners, customers, governors, associates, partners, sub-contractors and any other colleagues.

- Provide guidance on implementing the NCG Data Protection Policy and processing personal data in compliance with data protection legislation and with respect for confidentiality.

The GDPR is a UK regulation on data protection and privacy that sets guidelines for the collection and processing of personal information. When the UK left the European Union in 2020, the EU-GDPR was amended and written into UK law as the UK-GDPR.

The Data Protection Act 2018 sets out the data protection framework in the UK and should be read in conjunction with the GDPR. It updates and replaces the previous legislation and came into effect on 25<sup>th</sup> May 2018.

Data protection laws exist to strike a balance between the rights of individuals to privacy and the ability of organisations to use data for legitimate business purposes.

We are required to inform the Information Commissioner of each legal entity within NCG that acts as a data controller. Responsibility for maintaining these notifications rests with the Data Protection Officer.

### **3. Common Law Duty of Confidence**

The common law of confidentiality is a broad principle of law that prevents a person who receives information from another party in confidence from taking advantage of it. That person must not make use of it to the prejudice of the person who gave the information without obtaining their consent.

A duty of confidence arises when one person discloses information to another (for example employee to employer) in circumstances where it is reasonable to expect that the information will be held in confidence. It is a legal obligation derived from case law and included in professional codes of conduct. When an individual has died, information relating to that individual remains confidential under the common law.

Confidential information is not confined to personal data, which is the only remit of the Data Protection Legislation. For example, commercial contracts are usually confidential as are exam papers (at least until the exams have been taken). NCG also implements Non-disclosure Agreements, Data Processing Agreements and Data Sharing Agreements to this end.

### **4. Roles and Responsibilities**

The Chief Executive Officer has overall accountability and responsibility for data confidentiality and protection. Operational responsibility is delegated to the data protection lead and the Chief Executive is responsible for ensuring that the role is performed. The responsibilities of the individual or individuals undertaking the role must be formally documented when appointments are made. The data protection lead must also be adequately trained in order to perform the role.

All Employees are under legal and contractual obligations to keep personal and other information confidential not only during their employment (or equivalent) but also after it has been terminated.



## 5. Data Protection Principles

NCG shall process data in accordance with current data protection legislation the Data Protection Principles.

Data Protection Principles	How NCG Complies
Lawfulness, fairness and transparency	NCG issues Privacy Statements to its staff, students and customers explaining how it processes data at the point of capture and for what purposes.
Purpose limitation	NCG shall only use personal data for the purposes for which it was collected.
Data minimisation	NCG shall only collect personal data relevant to the purpose for which it is required.
Accuracy	NCG shall ensure the data it processes is correct, up to date and able to be rectified promptly.
Storage limitation	NCG shall not store data for longer than it is required.
Integrity & confidentiality	NCG implements various measures to protect personal data from unauthorised access, loss or destruction.

All employees are responsible for ensuring that the Data Protection Principles are observed at all times and at all stages of the lifecycle of the data including:

- Collection or capture of personal data
- Post collection processing of data e.g. storing, alteration, transmission etc.
- Erasure or destruction of personal data

NCG is required by law to be able to demonstrate compliance with the Data Protection Principles.

## 6. Records of Processing Activities

Article 30 of GDPR requires organisations to document all processing. This helps demonstrate compliance with data protection legislation. This is usually recorded in a data-mapping document. These records are managed by the Data Protection Team who will work with you to complete this documentation.

## 7. Lawful Basis for Processing Personal Data

In order to process Personal Data lawfully, we must meet one of the lawful bases for processing. The lawful basis must be established before processing begins. The six lawful bases are:

- **Consent:** The organisation shall be able to demonstrate that the data subject has provided recent, clear, explicit and defined consent for their data to be processed for a specific purpose.
- **Contract:** The 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.

- **Legal Obligation:** The processing is necessary for compliance with a legal obligation to which NCG is subject.
- **Vital Interest:** The processing is necessary in order to protect the vital interests of the data subject or of another natural person. E.g. to protect an individual's life.
- **Public Interest:** The processing is necessary for NCG to perform a task in the public interest or for official functions and the task or function has a clear basis in law. **Legitimate interest:** The processing is necessary for the organisation's legitimate interests. This condition does not apply if there is a good reason to protect the individual's personal data that overrides the legitimate interest.
- **Legitimate Interest:** The processing is necessary for the purpose of the legitimate interests of NCG or 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.

To process Special Category data NCG is required to have:

- An additional legal basis for processing under GDPR Article 9
- An appropriate policy document in place.

To meet this requirement, NCG has established conditions for processing in the NCG Special Category and Criminal Convictions Data Policy.

## 8. Deciding on the Appropriate Condition for Processing

If you are assessing the lawful basis for processing data, you must first establish that the processing is necessary. This means the processing must be a targeted, appropriate way of achieving the stated purpose. You cannot rely on a lawful basis if you can reasonably achieve the same purpose by some other means.

Remember that more than one basis may apply, and you should rely on what will best fit the purpose, not what is easiest.

Contact the Data Protection Team for advice regarding the lawful basis for process Personal Data in your area of responsibility.

## 9. Rights of the Data Subject

The GDPR ensures that individuals have rights regarding the way organisations handle their data and NCG must ensure all procedures that involve the processing of personal data can demonstrate how individuals can exercise these rights.

Individuals can request to exercise these rights verbally or in writing. The NCG Data Subject Rights Request template is available in [Appendix 1 for this purpose](#).

When a request to exercise any of the following rights is received by a member of staff, they must inform the Data Protection Team immediately.

### The Right to be Informed

- Individuals have the right to be informed about the collection and use of their personal data.

- NCG provides Privacy Notices to meet this requirement.

### **The Right of Access**

- Individuals have the right to request access to their personal data.
- This is often called a Subject Access Request

### **The Right to Rectification**

- Individuals have the right to have inaccurate personal data rectified or completed if it is incomplete.

### **The Right to Erasure**

- Also known as the right to be forgotten, this enables individuals to request their data be erased.
- This is not an absolute right and only applies in certain circumstances.

### **The Right to Restrict Processing**

- Individuals have the right to request the restriction or suppression of processing of their personal data.
- This is not an absolute right and only applies in certain circumstances.
- When processing is restricted, you are permitted to store the personal data, but not use it.

### **The 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.
- The right only applies to information an individual has provided to a Controller.
- It allows them to move, copy or transfer personal data easily from one IT environment to another in a safe and secure way, without affecting its usability.
- The right only applies to data that is processed by automated means (i.e. excluding paper)

### **The Right to Object**

- This gives individuals the right to object to the processing of their personal data in certain circumstances.
- Individuals have an absolute right to stop their data being used for direct marketing.
- In some cases, where the right to object applies NCG may be able to continue processing if there is a compelling reason for doing so.

### **Rights in relation to Automated Decision Making and Profiling**

- Automated decision making is using solely automated methods without any human involvement in order to make a decision about an individual.

- Profiling is any form of automated processing that uses personal data to analyse or evaluate certain personal aspects relating to an individual.

Organisations can only carry out this kind of processing if the decision is:

- Necessary for the entry into or performance of a contract.
- Authorised by domestic law applicable to the data controller.
- Based on the individual's explicit consent.

In order to process data in this manner, NCG shall ensure that:

- Individuals receive information about the processing.
- There are simple ways for the individual to request human intervention or challenge a decision.
- Regular checks are carried out to make sure that the systems are working as intended.

## **10. Privacy Statements**

Personal data must be processed 'in a transparent manner'. This is achieved by providing the data subject with information at the point of data capture, or if this is not possible, within a reasonable period after obtaining the data, but at least within one month. This information is known as a Privacy Statement, Privacy Notice or Privacy Policy.

NCG's Privacy Statements shall comply with the Regulation and follow the relevant ICO guidance including but not limited to:

- At the point of capturing an individual's data, NCG shall notify them of the ways in which their personal data may be held and processed.
- Where NCG relies on the consent of the Data Subject, a record of this consent must be maintained; in the case of special categories of personal data such consent must be explicit.
- Where the processing is for marketing purposes, the notification will highlight any opportunities to opt out of such communication. See Privacy Electronic Communications Regulations below for more information on marketing.
- If staff collect information about learners, customers or others, they must comply with the guidelines set out in these procedures and the data should not exceed the general information needs.
- NCG will notify new employees and governors that their personal data will be processed for employment purposes prior to the employment contract being signed.
- Learners and customers will be notified about the processing of their personal data and any opt-outs prior to signing their Learning Agreement, Enrolment Form or alternative document specified in the relevant contract.

Special Category data can only be collected and processed if the appropriate legal conditions are met. Staff needing to collect special category information must ensure they have authorisation by NCG to do so. The only exception is if a non-authorized member of staff is satisfied that the processing of the data is necessary in the vital interests of the learner, customer, staff member, or others. This exception is only applicable in limited circumstances such as medical emergencies.

The standard form for recording express consent is in Appendix 2.

The standard form for recording consent for images to be stored in media libraries and included in publications and publicity materials is in Appendix 3.

## 11. Privacy and Electronic Communications Regulations

The Privacy and Electronic Communications Regulations places further obligations on NCG when sending out electronic marketing communications. The recipients of electronic marketing communications are broken down into the following categories:

- Individual Consumers (including sole traders) i.e. personal contact details such as telephone number, email address, home address etc.
- Corporate Subscribers (business to business) i.e. an individual's work email address, work telephone number, work address etc.

In order to send direct marketing to an Individual Consumer, NCG **must** be able to evidence that the data subject has given their explicit consent to market to them. In order to send direct marketing to a Corporate Subscriber, there is no requirement to evidence consent as it is considered as a 'legitimate interest'.

When contacting both Individuals or Corporate Subscribers for marketing purposes, staff must always include, a link to or a copy of a privacy notice in every communication, as well as give the recipient the opportunity to 'opt out' of receiving any future communications. In terms of email communications, this can be done by adding in an 'Unsubscribe' link in the footer of any emails, or a statement advising that they can reply 'STOP' to unsubscribe. If an individual wishes to opt-out i.e. exercise their 'right to object' to direct marketing, this is their absolute right and therefore staff must ensure that no further marketing communications are sent to them.

The table in [Appendix 4](#) is taken from the ICO's guidance on direct marketing and should be used as a basis when deciding if it is acceptable to send out electronic marketing communications.

## 12. Data Protection Impact Assessments

A Data Protection Impact Assessment (DPIA) is an exercise used to help identify and minimise the data protection risk of a project. It shall:

- Describe the nature, scope, context and purposes of the processing.
- Assess necessity, proportionality and compliance measures.
- Identify and assess risks to individuals.

- Identify any additional measures to mitigate those risks.

A DPIA shall be carried out for the processing of any personal data that is likely to result in a high risk to individuals. The ICO requires organisations to conduct a DPIA in certain circumstances, but it is also good practice to do a DPIA for any other major project that requires the processing of personal data.

Contact the Data Protection Team for assistance when completing DPIAs.

### 13. Document Retention

The GDPR does not dictate how long you should keep personal data however, the 5<sup>th</sup> data protection principle states that “*data should be kept in a form which permits identification of a data subject for no longer than is necessary.*” This means that the data must only be stored for as long as it is required. NCG shall determine the suitable retention period for data being processed and ensure that once this data has reached this threshold, it is securely destroyed, anonymised or erased. The retention period of the data will be determined by the purpose for which it is processed and the lawful basis for processing it.

For data processed by NCG, the retention period and relevant justifications are recorded in the NCG Document Retention Schedule. It is the responsibility of relevant management to ensure that both paper and electronic records are retained or disposed of accordingly.

### 14. Criminal Offence Data

Article 10 of GDPR sets out high-level conditions for the processing of personal data relating to criminal convictions and offences. DPA 2018 sets our specific conditions for such processing in Schedule 1. NCG will only process criminal offence data in accordance with the current data protection legislation.

DPA 2018 requires that:

- When the processing is carried out, the controller has an appropriate policy document in place. To meet this requirement, NCG has established conditions for processing in the NCG Special Category and Criminal Convictions Data Policy.
- Organisations record the lawful condition for processing such data. This shall be determined prior to any processing and shall be recorded in the relevant data mapping document and/or DPIA.

NCG shall not keep a comprehensive register of criminal convictions.

### 15. Data Protection Breaches

Any breach of this policy or of data protection legislation must be reported as soon as practically possible to [dpo@ncgrp.co.uk](mailto:dpo@ncgrp.co.uk). This means as soon as you have become aware of a breach. NCG has a legal obligation to report any data breaches to the ICO within 72 hours.



All members of staff have an obligation to report actual or potential confidentiality or data protection compliance failures. This allows NCG to:

- Investigate the failure and take remedial steps if necessary.
- Maintain a register of compliance failures.
- Notify the ICO of any compliance failures that are material either in their own right or as part of a pattern of failures.

Any member of staff who fails to notify of a breach or is found to have known or suspected a breach has occurred but has not followed the correct reporting procedures will be liable to disciplinary action.

Please refer to the NCG Information Security Incident Reporting Policy for our reporting procedure.



**Appendix 1 – Data Subject Rights Request Form**

**Data Subject Rights Request Form**

You should complete this form if you wish to express one of your data subject rights as stated within the UK General Data Protection Regulation (GDPR). We will endeavour to respond promptly and in any event within one month of the latest of the following:

- On receipt of your written request; or
- On receipt of any information requested to confirm your identity.

Also, in order to assist NCG to locate the relevant information in a timely and efficient manner, you should provide as much information as possible as to:

- the type of data in question,
- the period during which the data has been held,
- the persons or departments who are likely to be holding this data
- and the sites and/or specific locations where such persons or departments are based.

The information you supply in this form will only be used for the purposes of identifying the relevant personal data and responding to your request. You are not obliged to complete this form to make a request, but doing so will make it easier for us to process your request quickly.

**SECTION 1: Details of the person requesting information**

Full name:	
Address:	
Telephone no:	
Mobile no:	
E-mail:	



**SECTION 2: Are you the data subject?**

Please place an ‘X’ in the appropriate box and read the instructions that follow it.

- YES: I am the data subject. I enclose proof of my identity (see below).  
(Please go to section 4)

- NO: I am acting on behalf of the data subject. I have enclosed the data subject’s written authority and proof of the data subject’s identity and my own identity (see below). (Please go to section 3)

To ensure we are communicating with the right person we require you to provide us with proof of your identity and of your address. Please supply us with a photocopy or scanned image (do not send the originals) of one or both of the following:

1) Proof of Identity (passport, photo driving licence, national identity card, birth certificate).

2) Proof of Address (utility bill, bank statement, credit card statement (no more than 3 months old); current driving licence; current TV licence; local authority tax bill, HMRC tax document (no more than 1-year-old).

If we are not satisfied you are who you claim to be, we reserve the right to refuse to grant your request.

**SECTION 3: Details of the data subject (if different from section 1)**

Full name:	
Address:	
Telephone no:	
Mobile no:	
E-mail:	

**SECTION 4:** Please place an 'X' the appropriate box to indicate which of your data subject rights you wish to express:

- Right of Access (Subject Access Request)
- Right to Data Portability
- Right to Object
- Right to Restrict Processing
- Right to Erasure
- Right to Rectification

**SECTION 5:** Details of your request:

Please provide as much detail as possible about your request in order to help us to identify the information you require.

We will usually automatically search the following sections for personal data: MIS, Finance, HR and any programme area in which you have studied or worked, as applicable. Please state below any other sections/departments that you have been in contact with that you would like to be searched for relevant data. If you wish to see only certain specific document(s), for example a particular examination report or a specific department file etc., please describe below:

Please note that if the information you request reveals details directly or indirectly about another person, we will have to seek the consent of that person before we can let you see that information. In certain circumstances, where disclosure would adversely affect the rights and freedoms of others, we may not be able to disclose the



information to you, in which case you will be informed promptly and given full reasons for that decision. There may be other relevant exemptions under the Data Protection Act 2018 that prevent NCG disclosing information to you. While in most cases we will be happy to provide you with copies of the information you request, we reserve the right in accordance with Article 12 of the GDPR to charge a fee or refuse the request if it is considered “manifestly unfounded or excessive”. However, we will make every effort to provide you with a satisfactory form of access or summary of information if suitable.

**SECTION 6: (To be completed for a Request for Data Portability)**

Please tick the appropriate box to indicate the format that you would like us to use to transmit the requested data:

- Microsoft Office (Word, Excel etc.)

- OpenDocument

– PDF

Other (Please Specify):

---

Please note that it may not always be possible to transmit your data in your requested format, however we will notify you of this prior to sending.

**Declaration**

I, ..... certify that the information given on this application form to NCG is true. I understand that it is necessary for NCG to confirm my identity and it may be necessary to obtain more detailed information in order to locate the correct information.

**Signed:** ..... **Date:** .....



The following must accompany this application:

- Evidence of identity, e.g. photocopy of driving licence or birth certificate

Please return the completed form and accompanying items to:

NCG Data Protection Officer, NCG, Rye Hill Campus, Scotswood Road, Newcastle upon Tyne NE4 7SA

Or via email to [dpo@ncgrp.co.uk](mailto:dpo@ncgrp.co.uk)

---

**Office Use Only:**

Date request received:

Notes:

Date completed:

Confirmed (signature):



**Appendix 2 – NCG Consent Form**

NCG Consent Form

\*Name:

\*Student ID number/Staff Payroll number:

Address:

Telephone number:

Email Address:

**(Insert/delete data types as required. Items marked with a \* are mandatory)**

I consent for the personal data above to be: **(delete as applicable)**

- Processed by NCG
- Disclosed to third parties including.....

For the following purposes:

- 1.
- 2.
- 3.
- 4.
- 5.

I understand that I have the right to withdraw my consent at any time and can do so by contacting **[insert contact details]** or NCG's Data Protection Officer via [dpo@ncgrp.co.uk](mailto:dpo@ncgrp.co.uk)

Signed.....  
Date.....

**Appendix 3 – Approval Form (Photograph, Quote, Film)**

Approval Form  
(Photograph, Quote, Film)

If the participant is considered a 'vulnerable person', their involvement must be discussed in advance with the appropriate safeguarding lead.

**Section A – to be completed at the outset by the participant**

Name:

Address:

Telephone number:

E-mail:

Name of Course/Programme:

Year: 1 2 3

Are you an employee, learner, customer, parent/guardian or other? (Please state):

Quote (if relevant):

I confirm that NCG are permitted to use photographs, quotes and film footage of myself in ANY/ALL publicity material (The organisation comprises Newcastle College, Newcastle Sixth Form College, West Lancashire College, Kidderminster College, Carlisle College, Lewisham College and Southwark College). I understand that I have no interest in the copyright or any moral rights in any of the above and shall not be contacted again for permission of usage. I understand that the choice of what is used is solely up to NCG and that when issued/printed it may be used as seen fit in prospectuses, press releases and other publicity materials. I understand that I have the right to withdraw my consent for the use of the material I have provided, however it is not possible for NCG to cease use of the material that is already printed or made publicly available prior to my withdrawal. If photos &/or quotes are sent to the media, I understand that they may use these as and when they think it is appropriate and I understand that I have no interest in this. I am 16 years of age or over.



Signed: ..... Date: .....

-----  
-----

**Section B - for NCG internal use**

Date of shoot/quote:

Location:

Description of model for identification:

Photographer/Operative/Marketing Department Representative:

Appendix 4 – ICO Guidance on Direct Marketing

Data protection | Privacy and Electronic

## At-a-glance guide to the marketing rules

Method of communication	Individual consumers (plus sole traders and partnerships)	Business-to-business (companies and corporate bodies)
Live calls	<ul style="list-style-type: none"> <li><input type="checkbox"/> Screen against the Telephone Preference Service (TPS)</li> <li><input type="checkbox"/> Can opt out</li> <li><input type="checkbox"/> Consumer must have given caller specific consent to make marketing calls about claims management services</li> <li><input type="checkbox"/> Pension schemes calls only if authorised and have consent or meet existing customer criteria</li> </ul>	<ul style="list-style-type: none"> <li><input type="checkbox"/> Screen against the Corporate Telephone Preference Service (CTPS)</li> <li><input type="checkbox"/> Can opt out</li> <li><input type="checkbox"/> Consumer must have given caller specific consent to make marketing calls about claims management services</li> </ul>
Recorded calls	<ul style="list-style-type: none"> <li><input type="checkbox"/> Consumer must have given caller specific consent to make recorded marketing calls.</li> </ul>	<ul style="list-style-type: none"> <li><input type="checkbox"/> Consumer must have given caller specific consent to make recorded marketing calls.</li> </ul>
Emails or texts	<ul style="list-style-type: none"> <li><input type="checkbox"/> Consumer must have given sender specific consent to send marketing emails/texts.</li> <li><input type="checkbox"/> Or soft opt-in (previous customer, our own similar product, had a chance to opt out)</li> </ul>	<ul style="list-style-type: none"> <li><input type="checkbox"/> Can email or text corporate bodies</li> <li><input type="checkbox"/> Good practice to offer opt out</li> <li><input type="checkbox"/> Individual employees can opt out</li> </ul>
Faxes	<ul style="list-style-type: none"> <li><input type="checkbox"/> Consumer must have given sender specific consent to send marketing faxes</li> </ul>	<ul style="list-style-type: none"> <li><input type="checkbox"/> Screen against the Fax Preference Service (FPS)</li> <li><input type="checkbox"/> Can opt out</li> </ul>
Mail	<ul style="list-style-type: none"> <li><input type="checkbox"/> Name and address obtained fairly</li> <li><input type="checkbox"/> Can opt out</li> </ul>	<ul style="list-style-type: none"> <li><input type="checkbox"/> Can mail corporate bodies</li> <li><input type="checkbox"/> Individual employees can opt out</li> </ul>



20190109  
Version 2.4