Writing a Data Protection policy or other Data Protection document

1 Introduction

The first and most important thing to work out with your Data Protection policy is the answer to a simple question: WHAT IS IT FOR? What purpose does it serve? What difference does writing and adopting it make to the organisation? Many DP policies regurgitate the principles and affirm the organisation's commitment to complying with it, but don't actually achieve anything else.

It is possible that you will adopt single a Data Protection Policy, or a single document of another kind, and that will be the only DP resource that your staff will need. It is more likely that you might achieve your objectives with a group of smaller documents – security and data quality procedures for everyone, and other procedures or documents that apply in specific situations. This is 2040's recommendation.

2 What your DP policy can do:

- Assign responsibility for data protection activities and decisions
- Record important decisions about how the organisation will approach Data Protection – GDPR requires an organisation to demonstrate compliance, so important decisions can be recorded within a corporate policy
- List requirements that you wish to place on staff (e.g. data sharing or security procedures)
- Record a corporate commitment to Data Protection or specific aspects of it if that will help

3 What your DP policy should be:

The policy **should** be

- Properly communicated – everyone covered by the policy must be aware of its existence. There is no point in setting out a policy if staff or others do not know what is says, or that it even exists

- Practical – you must not require your staff to do anything that is impractical or impossible; if there are practical steps that you expect people to follow, actions that you want them always to take, or never to take, those practical steps must be spelled out explicitly

- Understandable – the language needs to be simple, clear and approachable; if there are consequences or sanctions for not following the policy's requirements, these should be spelt out clearly and simply.

- Relevant – a policy should not contain any information that is not strictly necessary to do the job your policy is designed to do. It should not cover material that the intended audience do not need to know.

- Available – the policy needs to be visible to all staff that are covered by it

You need to think about the effect you want the document to have. It might be helpful to think about a number of different types of document and decide how your objective is best met. If you feel that your organisation needs an explicit corporate commitment to complying with Data Protection law, there is nothing wrong with that. However, if you're going to write and disseminate a policy, you should also make sure it has some sort of practical effect, so think about whether making that kind of corporate commitment will change anything within the organisation.

Policy: Sets out the organisation's position or approach on matters over which it has a choice i.e. we have decided to do these things

Procedure: Sets out the process that must be following: how a thing is done, an instruction to do this, don't do that. A procedure may set out exactly how a subject access request will be carried out, or it may give specific instructions about how to send sensitive information out of the organisation. We recommend that you have documented procedures in at least the following areas:

- incident reporting inside the data controller
- incident investigation
- dealing with subject rights

Guidance: Helpful information for situations where staff have discretion, or where rules are impossible. For example, guidance may contain advice about what factors a staff member may need to take into account when they receive a request for disclosure from the police. Guidance will not tell the reader what to do – it will give them information that will help them to make a decision.

4 What your Data Protection Policy could contain

Do not stuff your policy with information that not everyone needs to know. A policy that applies to all staff should only contain information that every member of staff needs to read. If there are instructions or requirements for specific members of staff or groups of staff, make them part of a separate document or an appendix that only those specific people need to know. For example, technical security measures or processes for access to CCTV images by third parties are likely only to be relevant to a limited number of people.

Every staff member needs to know that individuals have a right of subject access. You need staff to record personal data knowing that it might be accessed by the subject (e.g. so they don't call someone a 'moron' in an email). However, unless it is your policy that subject access requests will be devolved to individual staff and teams, rather than coordinated from the centre, not everyone needs to know how a request will be dealt with in detail. This might be better explained to them when a request actually arrives. Every member of staff needs to know the practical security requirements that apply to them when taking data out of the office; only those working in IT security need to know about specific back-up processes.

4.1 Possible elements

What this policy is for

Tell staff what the purpose of the document is, why you're asking them to read it and most importantly, anything you want to them do having read it, or anything that will happen as a result of them reading it. For example, if you're using it as a training tool, explain that and ask them some questions to test whether they understood it.

What happens if you don't follow it

If you are setting out steps that staff have to take, you need to be clear about what will happen if they fail to follow the policy. If there are direct consequences for violating the policy, make that clear.

Explain how the Data Protection Principles relate to your work

One effective approach is to list the DP principles, but then relate them to practical steps that need to be taken within the organisation. So rather than saying 'this is what GDPR says', the policy takes the form of 'GDPR says this, and in order to make this work, we need to make sure that we do these things.

For example, you would describe the transparency element of the first principle and then set out the practical steps required to make it work e.g. ensure transparency by ensuring that every application form includes a privacy notice and links to wider published privacy policies, ensure accuracy by reminding people at regular intervals to keep their data up to date and so on.

Data Protection Risks

You may wish to set out specific risks and issues that you want them to be aware of, and processes you wish them to follow in order to avoid them. You will need specific procedures for carrying out impact assessments, and alerting all staff to the benefits of risk-assessing new or changing processing may be an effective way to help with the drive to carry out impact asssessments.

Individual responsibilities

One of the most useful things to do in your policy is to set out who is responsible for what within the organisation. We recommend ensuring that your data protection policy includes the following roles

- Identity of the DPO or DP lead, and what they are required to do, what staff are required to do in order to assist them and (most importantly) when and how they should be consulted
- Identity and duties of the IT Security lead
- Senior Information Risk Owner (for larger organisations)
- Responsibilities of senior management team, including the extent of personal liability
- Responsibilities of departmental / team managers, e.g. ensuring staff follow security or data quality procedures, ensuring that procedures are followed when a staff member joins or leaves their team
- Responsibilities of staff, e.g. reporting incidents, assisting with subject access requests
- Processes for contractors, temps and volunteers e.g. ensuring that they sign confidentiality agreements, or do not store data on their own equipment after their work has ended

5 Areas suitable for policies and procedures

A single document that dealt with more than a few of the issues would be enormous, so if you believe your organisation would benefit from implementing rules or standards, you should split them up into a series of more manageable items. We are not suggesting that you must document all of these issues or govern them with fixed rules. These are areas where written rules and procedures tend to work, but there is more than one way to control information, and you need to decide what will fit best in the culture of your organisation.

Rules for staff conduct

Under both Data Protection and Human Rights law, failing to inform people about how their data will be used and what monitoring they will be subject to. For example, the Bărbulescu case from 2017 stressed the importance of staff being informed about rules governing their behaviour at work, but also the nature and extent of monitoring. Mr Bărbulescu won a breach of privacy case on this basis. Clear rules for the acceptable use of internet and devices, vehicles and equipment, as well as a description of how such rules will be monitored and enforced.

Security rules

- Identifying and reporting security incidents within the organisation – we recommend having a clearly identified single point of contact, and nominated officers to investigate
- Assessing the risks associated with an incident (for decision-makers involved in the process rather than all staff)
- Security questions to check the identity of people calling into the organisation, and their entitlement to data
    - For clients / customers, we recommend using information that a person is likely to know about their account or relationship with your organisation, rather than simply checking name, address and date of birth
    - For other data controllers calling to request information, we recommend getting all requests in writing so email addresses can be checked and time take to consider the request. Where that is not possible, we recommend calling the person back at a switchboard address, not any number they provide
- Procedures for working from home or on the move
- Procedures for sending data out of the office – we recommend using encrypted email or file transfer systems for special categories data, and other sensitive information like financial data
- Procedures when a staff member leaves (e.g. return of electronic devices, removing access to systems)
- Rules for the office (clear desk procedures, access controls for the building, dealing with visitors and strangers) – we recommend some form of clear desk policy for areas where sensitive data is processed
- Provisions for evaluating whether security measures are effective
- Approach to staff's own devices – if you operate a Bring Your Own Device approach, you need to ensure that staff's devices are encrypted, protected by a strong password, and there is a way to remotely wipe them. If the device is lost, they must report this as a matter of urgency. If you cannot

enforce the above rules, you need to ensure that devices can only be used for remote access, and that no data will be stored on the device.

- Secure disposal of personal data
- Building clearance procedure – there have been multiple incidents of data being left behind in buildings or furniture over the years, and we strongly recommend documenting a clear process for checking that this has not happened

Specific processes

- Verification of personal data to ensure data quality
- Disclosure – when and how to disclose personal information
- Subject rights – how data will be located, who by and who will make decisions about what response applicants will receive
- Impact assessments – how they will be triggered, who will carry them out, when to consult the DPO
- Contractors / processors – what to include in a GDPR-compliant contract for a data processor

6 More information

If you would like to know more or for assistance with your approach to Data Protection, please contact Tim Turner

Website: www.2040training.co.uk
Email: tim@2040training.co.uk
Phone: 0750 8341090

2040 Training Limited, Courthill House, 60 Water Lane, Wilmslow, Cheshire, SK9 5AJ
Registered in England - Company Number: 6682698 – VAT Number: 155713606