Data Protection and Security for Digital Tools

DELEGATE HANDBOOK

VERSION DATE	NOTES	AUTHOR
September 2021		Emma Cooper

KAFICO

INFORMATION · GOVERNANCE · CONSULTANCY

1. INTRODUCTION

Today's session provided a lot of information on a very complex topic so well done!

This handbook will provide some useful resources to help you put it all into practice in your business.

Do remember that the training you have been provided is 'foundation' level and that there is much more detail available on the ICO website. As your organisation grows and the law changes and develops, you should continue to review your compliance and seek professional support when needed.

2. ITEMS WE DIDN'T COVER

We simply couldn't cover everything in three hours so here are some areas you should have read about when you start your compliance work and some resources to help you.

Selecting a Lawful Basis

You can read more about ensuring you have identified the lawful basis for processing personal data at;

https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/

Or visit www.ico.co.uk and search for "Lawful Basis for Processing".

Obtaining Lawful Consent

See Appendix A for a checklist you can use to help ensure your customer consent is lawful.

International Transfers

This is a very complex area of law, particulary now, as we settle post Brexit, and deal with some international court cases that have changed the approach.

The ICO provide some guidance at https://ico.org.uk/for-organisations/dp-at-the-end-of-the-transition-period/data-protection-and-the-eu-in-detail/the-uk-gdpr/international-data-transfers/

Or visit www.ico.co.uk and search for “International Transfers”

However, if your system supplier transfers data outside of the UK, it might be best to seek some specialist advice.

Sharing Between Controllers

During the session, we talked about how suppliers will often be processing on our behalf with very little autonomy and will therefore be Data Processors.

Some suppliers are actually Data Controllers in their own right. This is because they CAN exercise control. An example would be an accountant who will do their work according to HMRC rather than your instructions – although you pay them.

When you are both Controllers, make sure your commercial contract describes the information that will be shared, how it will be shared and looked after by the parties.

https://ico.org.uk/media/for-organisations/data-sharing-a-code-of-practice-1-0.pdf

Or visit www.ico.co.uk and search for “sharing between controllers”.

Appointment of a DPO

As a small organisation, it is likely that you are not required by law to have a Data Protection Officer (DPO) – although you should still nominate someone to oversee data protection.

The DPO role is a formal and skilled role. As your company or data volume grows, check whether your company now needs to appoint a DPO.

https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-officers/

Or visit www.ico.co.uk and search for “Data Protection Officers”

Data Protection Impact Assessments

Certain changes, such as introducing CCTV or the use of innovative technology like fingerprint door entry, requires you to complete an assessment of the impact the change will have on the privacy of data subjects.

To see whether any changes you are introducing might need an impact assessment, see our handy checklist at Appendix B.

The ICO provide some helpful guidance on how to complete Data Protection Impact Assessments at https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-

the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-impact-assessments/

Or visit www.ico.co.uk and search for “data protection impact assessments”.

3. RESOURCES FOR THE COURSE CONTENT

Lets get back to what you learned on the course! For each of the sections we covered, we have included some basic reminders and the resources to help you apply them in your day to day.

The ICO provide a comprehensive guide to help organisations to navigate data protection law at www.ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/.

https://ico.org.uk/for-organisations/guide-to-pecr/what-are-pecr/

We have also included some of the tools we mentioned during the session, below.

Registering with the ICO

You may need to register with the ICO.

To check if you are exempt or not, visit https://ico.org.uk/for-organisations/data-protection-fee/self-assessment/

Or visit www.ico.co.uk and search for “registration self-assessment”

Supplier Contracts

Where a provider or system supplier is going to process data on behalf of your organisation, you need to ensure that there is a contract in place that defines what they will and won'd do with the data you provide.

See Appendix C for a checklist to help you review contract.

System Set Up

When you are buying or setting up new systems, you will want to check that the security features match up with the risk posed by the data involved.

This means ensuring that Special Category Data, in particular, is protected by measures such as 2 factor authentication (sending a code as another part of logging in, for example).

Gov.UK Design provide some useful guidance about security measures for systems at https://design-system.service.gov.uk/patterns/passwords/

We have produced a simple checklist to help you feel confident that you have done the right checks on your new or prospective digital tool. See Appendix E.

It may also be helpful to ask the supplier to provide you with a "Privacy by Design" or "Technical and Organisational Measures" to assist you.

Some suggested wording for the request might be;

"I am completing some due diligence on the system and wondered if you might be able to provide your "Privacy by Design" or "Technical and Organisational Measures" that demonstrates how privacy and security has been built into the system and what the measures are."

Once you have a respond, you can use the checklist to make sure you are happy that the key security elements are in place.

Information Rights

The ICO provide some useful guidance that goes into more detail about the time limits and exceptions to the information rights at https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/

Or visit www.ico.co.uk and search for “individual rights”.

Email us at info@kafico.co.uk to obtain a template Information Rights Policy to amend and implement for your business.

Transparency

The law requires that certain items are included in your company privacy policy.

Appendix E is a useful checklist that you can use to review your privacy policy and support compliance.

APPENDIX A: CONSENT CHECKLIST

Valid Consent Criterion	Detail	Status
We have made the request for consent prominent and separate from our terms and conditions	*Example: We provide a clear tick box specifically for direct marketing purposes*	
We ask people to positively opt in.	*Example: individuals are required to ask to use tick box to say they are happy for information to be used this way.*	
We don’t use pre-ticked boxes or any other type of default consent.	*Example: individuals are required to complete a consent form and tick to say they are happy for information to be used in this way.*	
We use clear, plain language that is easy to understand.	*Example: Where appropriate our materials are easy to read, pictorial and video form as well as written text. Other languages are available where deemed necessary.*	

We specify why we want the data and what we're going to do with it.	*Example: individuals are provided with a list of specific activities we undertake using their data*	
We give individual ('granular') options to consent separately to different purposes and types of processing.	*Example: individuals are able to indicate what activities they are happy for us to use their data for and which they aren't. This can be recorded in local systems.*	
We name our organisation and any third-party controllers who will be relying on the consent.	*Example: Our privacy notices list all of our sharing partners specifically by name.*	
We tell individuals they can withdraw their consent.	*Example: contact details are provided for individuals to withdraw consent from any or all of the processing activities.*	
We ensure that individuals can refuse to consent without detriment.	*Example: Withdrawal of consent to marketing does not affect the individual's ability to access our services*	
We avoid making consent a precondition of a service.	*Example: Withdrawal of consent to these activities (marketing for example) does not affect the individual's ability to access our general services*	
If we offer online services directly to children, we only seek consent if we have age-verification measures (and parental-consent measures for younger children) in place.	*Example: We deliver a health app that children can access. Age is verified through biometric authentication.*	
We keep a record of when and how we got consent from the individual.	*Example: Our system allows us to record when consent was obtained and upload consent forms.*	
We keep a record of exactly what they were told at the time.	*Example: The privacy information is version controlled. When a change is made to information flows, consent is obtained again by re-providing the privacy notice.*	
We regularly review consents to check that the relationship, the processing and the purposes have not changed.	*Example: Quarterly reviews of consents are undertaken to ensure that consent remains valid.*	
We have processes in place to refresh consent at appropriate intervals, including any parental consents.	*Example: Quarterly reviews of consents are undertaken to ensure that consent remains valid.*	
We consider using privacy dashboards or other preference-management tools as a matter of good practice.	*Example: Our system allows us to record granular levels of consent and to give effect to them through read codes.*	
We make it easy for individuals to withdraw their consent at any time and publicise how to do so.	*Example: Our staff are trained to action withdrawal of consent and the option is also available on our website.*	
We act on withdrawals of consent as soon as we can.	*Example: Our staff are trained to action withdrawal of consent and the option is also available on our website.*	
We don't penalise individuals who wish to withdraw consent	*Example: Withdrawal of consent does not affect the individual's ability to access services.*	

APPENDIX B: DATA PROTECTION IMPACT ASSESSMENT CHECKLIST

If you tick **any** of the sections below, the DPO should ***consider*** a DPIA.	
Evaluation or scoring of individuals	
Automated decision-making with significant effects	
Systematic monitoring (surveillance for example)	
Processing of sensitive data or data of a highly personal nature	
Processing on a large scale (Examples of large-scale processing include: a hospital (but not an individual doctor) processing patient data, tracking individuals using a city's public transport system; a fast food chain tracking real-time location of its customers; an insurance company or bank processing customer data; a search engine processing data for behavioural advertising; or a telephone or internet service provider processing user data.	
Processing of data concerning vulnerable data subjects (employees, children, people with impaired capacity)	
Innovative technological or organisational solutions	
Processing that involves preventing data subjects from exercising a right or using a service or contract	

If you tick **any** of the sections below, the project **requires** a DPIA.	
Systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person	

Processing on a large scale of special categories of data or of personal data relating to criminal convictions and offences	
Systematic monitoring of a publicly accessible area on a large scale	
Use profiling, automated decision-making or special category data to help make decisions on someone's access to a service, opportunity or benefit	
Combine, compare or match data from multiple sources	
Process children's personal data for profiling or automated decision-making or for marketing purposes, or offer online services directly to them	
Process personal data that could result in a risk of physical harm in the event of a security breach	

If you tick **TWO** of the sections below, the project **requires** a DPIA.	
Processing biometric or genetic data[1]	
Use of innovative technology[2]	
Processing personal data without providing a privacy notice directly to the individual	
Processing personal data in a way that involves tracking individuals' online or offline location or behaviour	

APPENDIX C: PROCESSOR CONTRACT CHECKLIST

[1] DNA, facial images, fingerprints, tissue samples

[2] Artificial intelligence, machine learning and deep learning; connected and autonomous vehicles; intelligent transport systems; smart technologies (including wearables); market research involving neuro-measurement (e.g. emotional response analysis and brain activity); some 'internet of things' applications, depending on the specific circumstances of the processing.

Required clause/areas covered by contract	Included y/n/NA	Notes/Comments
Is the processor required to provide, on request evidence that they have implemented appropriate technical and organisational measures to protect Personal Data including storage and transmission of data, business continuity, staff training, auditing, access control and Cyber security? **TIP: You will often find this clause by searching the term "technical" or "measures" in the contract.**		
Does the contract state that the processor shall not engage another processor without prior specific or general written authorisation of the controller? **TIP: You will often find this clause by searching the term "Sub" or "contractor" or "engage" in the contract.**		
Does the contract set out the subject-matter and duration of the processing, the nature and purpose of the processing, the type of personal data and categories of data subjects and the obligations and rights of the controller? **TIP: This is normally described at the bottom in a 'schedule' or appendix.**		
Does the contract stipulate that the Processor processes the personal data only on documented instructions from the controller, including with regard to transfers of personal data to a third country or an international organisation, unless required to do so by law and in those cases will notify the Controller? **TIP: You will often find this clause by searching the term "Instruction" or "instructed" in the contract.**		
Does the contract state that all staff employed by the processor have contracts that include confidentiality clauses and that Personal Data will not be shared with third party unless required to do so by law?		

TIP: You will often find this clause by searching the term "confidentiality" or "employees" in the contract.		
Does the contract require the Processor to assist the Controller to respond to requests for exercising the data subject's rights i.e. access to information, correction of errors? **TIP: You will often find this clause by searching the term "rights" or "requests" in the contract.**		
Does the contract require the Processor to assist the Controller in reporting information incidents promptly including where it might be required to contact the data subject? **TIP: You will often find this clause by searching the term "incident" or "breach" in the contract.**		
Does the contract state what should happen to the data at the end of the contract or in the event of termination such as return of the data or secure destruction? **TIP: You will often find this clause by searching the term "exit" or "return" or "destroy" in the contract.**		
Does the contract require the Processor to allow for a comply with audits including inspections conducted by the Controller or a third party engaged by the Controller? **TIP: You will often find this clause by searching the term "evidence" or "audit" in the contract.**		

APPENDIX D: PRIVACY POLICY CHECKLIST

Item	Present?
The name and contact details of our organisation.	
The contact details of our data protection officer (if applicable).	

The reason that we process personal data	
Our lawful basis for the processing personal data.	
The categories of personal data we process (personal / special category – name, address, DOB etc)	
Who we share the information with (including any suppliers)	
Any international transfers (which countries)	
How long we keep the data and if we de-identify at any stage	
The rights available to individuals in respect of the processing.	
The right to withdraw consent (if applicable).	
The right to lodge a complaint with the ICO	
How we received the personal data (they provided it? Collected automatically like cookies, from a third party etc)	
Any automated decision-making and / or profiling	

APPENDIX E: SYSTEM SUPPLIER CHECKLIST

We have thought about whether the system is a higher risk system (because it contains Special Category Data or is of high value to the running of our organisation)	
We have confirmed what we are a Data Controller, and the system provider is a Data Processor	
We have reviewed the contract against the Processor Contract Checklist to make sure all the Data Protection Clauses are present	
We have checked that the system provider does not send, access or host the data outside of the UK. If the data is transferred internationally, we have reviewed using the ICO's 'International Transfers' guidance to make sure it is lawful (www.ico.co.uk).	

We have queried with the supplier whether data is 'encrypted' in transit (as it moves between systems or over the internet). Ideally, it should be 'TLS v1.2 or above'[3]	
We have queried with the supplier whether the data is encrypted at rest (when it is just sitting within the system). Ideally, it should be 'AES 256' bit encryption.	
We have queried whether the system is protected by a firewall service (this protects your data from intruders).	
We have checked that there is a backup made of the data that we can retrieve if something goes wrong.	
We have queried with the supplier whether the system allows us to audit who has accessed the system	
The system allows individuals to log in individually. For high-risk systems, we have queried with the supplier whether we can activate a "two factor" authentication[4].	

[3] https://www.ncsc.gov.uk/collection/cloud-security/implementing-the-cloud-security-principles/data-in-transit-protection

[4] The system sends a code via email or text when people log in, for example