Law Enforcement processing (Part 3 of the DPA 2018)

Introduction

This part of the Act transposes the EU Data Protection Directive 2016/680 (Law Enforcement Directive) into domestic UK law. The Directive complements the General Data Protection Regulation (GDPR) and sets out the requirements for the processing of personal data for criminal 'law enforcement purposes' (LEP).

For international transfers, it also replaces the 2008 Council Framework Decision (2008/977/JHA) on the protection of personal data processed in the framework of police and judicial co-operation in criminal matters.

*(Part 2 of the Act covers aspects of the GDPR that allow for national derogations in specific instances. Part 2 also sets out the scope and definitions for **general processing** under the GDPR.*

Who does Part 3 apply to?

Part 3 applies to processing personal data for '**law enforcement purposes**', although it does not apply to all processing that we do.

It covers processing for the prevention, investigation, detection or prosecution of **criminal** offences, or the execution of **criminal** penalties, including the safeguarding against and the prevention of threats to public security.

So, it applies, but is not limited, to:

- the Police, criminal courts, prisons, non-policing law enforcement; and
- any other body that has statutory functions to exercise public authority or public powers for any of the law enforcement purposes.

Part 3 of the Act applies to both 'controllers' and 'processors' providing that the contract is for the purposes of processing personal data for the law enforcement purposes.

(A non-exhaustive list of 'competent authorities' that may use Part 3 is detailed in Schedule 7 of the Act.)

Any processing carried out by a 'competent authority' which is **not for the primary purpose of law enforcement** will be covered by the **GDPR and Part 2, Chapter 2 of the Data Protection Act**. For example, this may include internal HR processes and procedures, as that processing isn't strictly for law enforcement purposes. ***For clarification all Police Forces are deemed Competent Authorities.***

How is personal data defined?

Any information relating to an identified or identifiable **living** individual.

An identifying characteristic could include a name, ID number or location data. Such information is treated as personal data even if it can only be potentially linked to a living individual.

What is a 'controller'?

A controller determines how and why personal data is processed. For the purposes of law enforcement, this will be a competent authority which is acting alone, or jointly with others.

A processor processes personal data on behalf of the controller for the law enforcement purposes, but could be sharing some accountability with controllers. This means that a processor could be liable for breaches. Where Nottinghamshire police uses a processor, a processing contract is in place.

What is a 'competent authority'?

A competent authority for the purposes of law enforcement means a person specified in Schedule 7 and any other person if, and to the extent that, the person has **statutory functions to exercise public authority or public powers for the law enforcement purposes, or** where the authority have a **legal power to process personal data for law enforcement purposes**. For example, local authorities who **prosecute** *trading standards offences,* or the Environment Agency when prosecuting *environmental offences*.

What about sensitive processing?

In the context of law enforcement, the personal data we are processing will often be sensitive. When it is, we must be able to demonstrate that the **processing** is **strictly necessary** and satisfy **one** of the conditions in **Schedule 8** or is based on **consent**.

The Principles

The **six law enforcement principles under Part 3**, Chapter 2 of the Act are the main responsibilities we follow when processing personal data for law enforcement purposes.

- The principles are broadly the same as those in the GDPR, and are compatible across the two regimes.
- There are no principles relating to *individuals' rights or overseas transfers* of personal data - these are *addressed in the Act separately*.
- Transparency requirements are not as strict, due to the potential to prejudice an ongoing investigation in certain circumstances.
- We must be able to demonstrate overall compliance with all of the law enforcement principles.

What are the principles?

The first data protection principle

Processing of personal data for any of the law enforcement purposes must be lawful and fair.

The second data protection principle

The law enforcement purpose for which personal data is collected on any occasion must be specified, explicit and legitimate, and;

Personal data collected must not be processed in a manner that is incompatible with the purpose for which it was originally collected.

The third data protection principle

Personal data processed for any of the law enforcement purposes must be adequate, relevant and not excessive in relation to the purpose for which it is processed.

The fourth data protection principle

Personal data processed for any of the law enforcement purposes must be accurate and, where necessary, kept up to date, and;

Every reasonable step must be taken to ensure that personal data that is inaccurate, having regard to the law enforcement purpose for which it is processed, is erased or rectified without delay.

The fifth data protection principle

Personal data processed for any of the law enforcement purposes must be kept for no longer than is necessary for the purpose for which it is processed. Appropriate time limits must be established for the periodic review of the need for the continued storage of personal data for any of the law enforcement purposes.

The sixth data protection principle

Personal data processed for any of the law enforcement purposes must be processed in a manner that ensures appropriate security of the personal data, using appropriate technical or organisational measures (and, in this principle, “appropriate security” includes protection against unauthorised or unlawful processing and against accidental loss, destruction or damage).

What is the first principle about?

Fairness and lawfulness are well established requirements of data protection law. Any processing we carry out for the law enforcement purposes must be necessary.

In practice, the *lawful basis* would either be necessary for the performance of a task carried out for law enforcement purposes by a competent authority, or based on consent. There may be circumstances where we obtain consent from the individual whose data we are processing, although this will only be appropriate in certain circumstances in the context of law enforcement.

Many of the lawful basis for processing depend on the processing being *necessary*. This does not mean that processing always has to be essential. However, it must be a ***targeted and***

proportionate way of achieving the purpose. The lawful basis will not apply if you can reasonably achieve the purpose by some other less intrusive means.

It is not enough to argue that processing is necessary because one has chosen to operate their business in a particular way. The question is whether the processing is a ***necessary for the stated purpose.***

In terms of **consent**, this aligns with GDPR and it must be *unambiguous and involve a clear affirmative action*. (Further guidance on consent can be found in the ICO Guide to the GDPR).

'**Fairness**' generally requires us to be, where appropriate, *clear and open* with individuals about how we use your information, in keeping with your reasonable expectations.

'**Lawful**' processing means authorised by either *statute*, *common law* or *royal prerogative*, or by or under any other *rule of law*. It also meets one of the *conditions for processing* under Data Protection legislation. For example, Part 5 of the Police and Criminal Evidence Act 1984 confers statutory authority for the taking and retention of DNA and fingerprints (this applies to England and Wales). Also, the Domestic Violence Disclosure Scheme relies on the Police's common law powers to disclose information where it is necessary to do so to prevent crime.

What about sensitive processing?

In the context of law enforcement, the personal data we are processing will often be sensitive. When it is, we must be able to demonstrate that the processing is *strictly necessary* and satisfy *one of the conditions in Schedule 8* or is based on *consent.* Strictly necessary in this context means that the processing has to relate to a *pressing social need*, and we cannot reasonably achieve it through less intrusive means.

Sensitive processing is defined in the law enforcement provisions as:

(a) the processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs or trade union membership;

(b) the processing of genetic data, or of biometric data, for the purpose of uniquely identifying an individual;

(c) the processing of data concerning health;

(d) the processing of data concerning an individual's sex life or sexual orientation.

Genetic data is personal data relating to the inherited or acquired characteristics of a person, eg an analysis of a biological sample.

Biometric data is personal data that is obtained through specific processing relating to physical, physiological or behavioural characteristics of a person. This processing enables you to identify a particular person, eg DNA, fingerprints, and facial recognition.

Given the sensitivity surrounding such processing, we are required to meet at least one of the

conditions set out in Schedule 8 of the Act.

What safeguards are required for sensitive processing?

If we are carrying out sensitive processing based on the consent of a data subject, or based on another specific condition in Schedule 8 of the DP Act, we will have an appropriate *policy document* in place.

Our **policy explains**:

- our *procedures for complying with the data protection principles* when relying on a condition from Schedule 8; and
- our policy for the *retention and erasure* of personal data for this specific processing.

We will retain this policy from the time we begin sensitive processing until six months after it has ended. We will review and update it where appropriate and make it available to the Information Commissioner upon request without charge.

So when **processing sensitive personal data**:

- it must be strictly necessary;
- it must satisfy one of the conditions in Schedule 8; &
- there will be a policy document in place to demonstrate compliance, safeguards and processes.

What is the second principle about?

The second principle is about maintaining the *purpose for processing personal data*. Specific requirements about the purpose being **specified, explicit and legitimate** are introduced, meaning that any processing under Part 3 of the Act must be for the defined law enforcement purposes. We cannot process for a purpose that is incompatible with the original reason and justification for processing.

(For example, the Crown Prosecution Service could process personal data in connection with the prosecution of a criminal offence, whereas the Police working alongside the prosecutor would only be processing the personal data in connection with the investigation of the offence.)

What are principles three, four and five about?

The *third principle* requires that the personal data you are holding is **adequate** and **limited to** what is necessary for the purpose(s) you are processing it.

The *fourth principle* is about **accuracy**. It sets out that we should take every reasonable step to correct inaccurate data. In addition, **as far as possible**, we need to be able to distinguish

between personal data that is based on factual data and that which is based on a matter of opinion or assessment, such as a witness statement.

A new requirement under Part 3 is that again, where relevant, and as far as possible, we need to be able to distinguish data between **different categories of individuals**, such as suspects; individuals who have been convicted; victims and witnesses. Other unused data falls under the general provisions of GDPR and Part 2 of the Act.

The fifth principle requires that we **do not keep personal data for longer than is necessary** for the purpose we originally collected it for. We conduct regular reviews to ensure that we are not storing for longer than necessary for the law enforcement purposes.

What is the sixth principle about?

The sixth principle requires us to have **technical and organisational measures** in place to ensure that we protect data with an appropriate level of **security**. This is the same as under GDPR and Part 2 of the Act.

'Appropriate security' includes 'protection against unauthorised or unlawful processing and against accidental loss, destruction or damage'.

The **conditions for sensitive processing in Schedule 8** of the Act are:

- necessary for judicial and statutory purposes – for reasons of **substantial public interest**;
- necessary for the administration of justice;
- necessary to protect the vital interests of the data subject or another individual;
- personal data already in the public domain (manifestly made public);
- necessary for legal claims;
- necessary for when a court acts in its judicial capacity;
- necessary for the purpose of preventing fraud; and
- necessary for archiving, research or statistical purposes.

Again, we must be able to demonstrate that the processing is **strictly necessary** and satisfy one of the above conditions in Schedule 8 or is based on consent. Strictly necessary in this context means that the processing has to relate to a ***pressing social need***, and we cannot reasonably achieve it through less intrusive means.

Sensitive processing and Consent

Consent may not be appropriate in some circumstances and should only be used where the subject has a choice in relation to the proposed sensitive processing.

What are judicial and statutory purposes/administration of justice?

The sensitive processing must be necessary for the *administration of justice*, or the *exercise of a function conferred 'on a person' by enactment*. This covers a constable and other competent authorities including the Police.

In addition, in order to satisfy this condition, we must be able to demonstrate that the processing is necessary for reasons of substantial public interest.

When is processing appropriate for individual's vital interests?

This condition only applies in *cases of life or death*, such as if we disclose an individual's medical history to a hospital's A&E department who are treating them after a serious road accident.

What about personal data already in the public domain?

This condition applies if the data subject has deliberately made the information public.

What about legal claims and judicial acts?

This condition is met if the processing is necessary for the *establishment, exercise or defence of a legal claim* or whenever a *court* is *acting in its judicial capacity*.

When can data be processed for preventing fraud?

This condition can be used if the processing is necessary for the purposes of *preventing fraud*. If it involves sharing data with organisations that do not fall within the definition of a competent authority, the processing needs to comply with the applied GDPR elements in the DPA, and we need to have a lawful basis for sharing the data.

What about archiving?

This condition can be used if processing is necessary for *archiving in the public interest*; for *scientific or historical research purposes*, or for *statistical purposes*. However, we cannot use it if it will result in decisions being made that affects a particular individual, or is likely to cause substantial damage or substantial distress to an individual.

Categories of personal data

In all areas of policing and criminal justice, it is highly likely that any processing of personal data will involve different categories of data subject. When processing personal data for the any of the law enforcement purposes, we must provide, **where relevant and as far as possible**, a clear distinction between different **categories of personal data**, such as people who are:

- suspected of having committed, or about to commit, a criminal offence (suspects);
- convicted of a criminal offence;

- individuals who are, or are suspected of being, victims of a criminal offence (victims); or
- Individuals who are witnesses, or can provide information, about a criminal offence (witnesses).

There may be instances where an individual falls under more than one of these categories. For example an individual may be both a victim and a witness in a certain case, or indeed an offender in one case and victim/witness in another.

Under the fourth principle, we must ensure that any personal data we process for law enforcement purposes is accurate and, where necessary, up to date.

We will only categorise the information under Part 3 **where relevant** to the investigation, and any other unused data will fall under the general provisions of GDPR/ Part 2 of the Act.

Any unused personal data is also subject to strict retention periods.

We will also distinguish, so far as possible, any personal data based on facts from personal data based on personal assessment – i.e. distinguish between fact and opinion.

Privacy by Design

We will implement technical and organisational measures to show that we have considered and integrated data protection into your processing activities (privacy by design will be implemented where relevant).

What is data protection by design?

Under the GDPR and Part 3 of the Act, we have a general obligation to implement appropriate technical and organisational measures to show that we have considered and integrated the principles of data protection into our processing activities.

When processing personal data for law enforcement purposes, we will implement these measures by default, to ensure that we only process personal data for a specified and necessary purpose.

We must ensure that by default, we put safeguards in place to prevent personal data being made available to an indefinite number of people without an individual's intervention.

Data Protection Impact Assessment

A data protection impact assessment (DPIA) is 'an assessment of the impact of the envisaged processing operations on the protection of personal data'.
We carry out a DPIA before we process personal data when the processing is likely to result in a high risk to the rights and freedoms of individuals.

What is a data protection impact assessment?

Data protection impact assessments or DPIAs (previously known as privacy impact assessments or PIAs) are a tool that can help us identify the most effective way to comply with our data protection obligations and meet individuals' expectations of privacy. An effective DPIA allows us to identify and fix problems at an early stage, reducing the associated costs and damage to our reputation which might otherwise occur.

When do we need to conduct a DPIA?

We will carry out a DPIA before we process personal data when the processing is likely to result in a high risk to the rights and freedoms of individuals.

Processing that is likely to result in a high risk includes (but is not limited to):

- systematic and extensive processing activities, including profiling and where decisions that have legal effects, or similarly significant effects, on individuals;
- large scale processing of special categories of data or personal data relation to criminal convictions or offences;
- using new technologies (for example surveillance systems).

We will take into account the nature, scope, context and purposes of the processing when deciding whether or not it is likely to result in a high risk to individuals' rights and freedoms.

How do we carry out a DPIA?

A DPIA will contain:

- at least a general description of the processing operations and the purposes;
- an assessment of the risks to the rights and freedoms of individuals;
- the measures envisaged to address those risks;
- the safeguards, security measures and mechanisms in place to ensure you protect the personal data; and
- a demonstration of how you are complying with Part 3 of the Act, taking into account the rights and legitimate interests of the data subjects and any other people concerned.

When do we need to send our DPIA to the ICO?

If we have carried out a DPIA that identifies a high risk and cannot take any measures to reduce this risk, we need to consult the ICO and cannot go ahead with the processing until we have done so.

The focus is on the 'residual risk' after any mitigating measures have been taken. If our DPIA

identified a high risk, but we have taken measures to reduce this risk so that it is no longer a high risk, we do not need to consult the ICO.

Transfers

- Part 3, Chapter 5 deals with when we can transfer personal data to a **third country**.
- A third country is not an EU Member State, and the Act places limits on the circumstances when we can share.
- We have to meet certain conditions, including if the transfer is for one of the law enforcement purposes set out in Part 3.
- Mostly, we can transfer to a **'relevant authority'** - a body entrusted with similar law enforcement responsibilities in the third country.
- There are specific provisions if we transfer to bodies that are not relevant authorities, with additional requirements which we must meet before we can do this.

What are the general principles for the transfer of personal data?

There are three conditions that we have to meet before we can make a transfer:

- The transfer has to be necessary for any of the law enforcement purposes.
- The transfer has to be based on either a finding of adequacy in respect of the third country, or where other appropriate safeguards are in place, or if not, that the transfer is for certain specified special circumstances.
- The transfer is to a relevant authority in the third country, or is a 'relevant international organisation' ie an international body that carries out functions for any of the law enforcement purposes.

However it is still possible to transfer personal data to a body which is not a relevant authority, if we meet certain additional safeguards.

If the data is obtained from a competent authority in another EU member State, then that competent authority has to authorise the transfer. Except if:

- there is an immediate and serious threat to the public security of a member State or third country;
- there is an immediate and serious threat to the essential interests of a member State; and
- authorisation cannot be obtained in good time.

In such cases the relevant competent authority which would have been responsible for authorising the transfer, must be informed without delay.

Can we make a transfer subject to appropriate safeguards?

We may transfer personal data if the organisation who receives it has provided adequate

safeguards. As with the transfer of personal data under the GDPR, it will be sufficient if there is:

- a current finding of adequacy by the European Commission for the data protection provisions of the third country, or specified and relevant sectors within the third country; or
- a finding that the relevant international organisation offers an adequate level of data protection.

Otherwise, we may make the transfer on the basis that adequate safeguards exist to ensure that individuals' rights are enforceable and effective legal remedies for individuals must be available following the transfer.

Adequate safeguards may be provided for by:

- a legal instrument providing appropriate safeguards which binds the intended recipient; or
- an assessment performed by the data controller which concludes that appropriate safeguards exist. In this case, we must inform the Information Commissioner of the categories of data transfers that take place.

There is a requirement for us to document transfers and provide this documentation to the Information Commissioner on request, including:

- the date and time of the transfer;
- the name, and any other pertinent information about the recipient;
- the justification for the transfer; and
- a description of the data we transferred.

We must ensure that any personal data We have transferred is not further transferred to another third country without our authorisation, or another competent authority, and any authorisation can only be given where the transfer is necessary for any of the law enforcement purposes.

Are there any special circumstances?

Sometimes, we may need to transfer personal data when there is neither a finding of adequacy, nor appropriate safeguards in place. This can only take place in certain, specified circumstances, referred to as the 'special circumstances'. These are listed in the Act as the five circumstances where the transfer is necessary:

1. To protect the vital interests of the data subject or another person;
2. To safeguard the legitimate interests of the data subject;
3. For the prevention of an immediate and serious threat to the public security of a member state or third country;
4. In individual cases for any of the law enforcement purposes; or
5. In individual cases for a legal purpose.

We need to document the transfer, and provide those records to the Information Commissioner on request. We must record:

- the date and time of the transfer;
- the name, and any other pertinent information about the recipient;

- the justification for the transfer; and
- a description of the personal data we transferred.

These are the same details that we are required to record for transfers on the basis of appropriate safeguards.

Can we make a transfer to recipients other than relevant authorities?

For the most part, it is expected that transfers will take place between 'relevant authorities', or relevant international organisations ie any (legal) person in the third country (or operating internationally) who has functions comparable to those of a 'competent authority' for the purposes of Part 3 of the Act.

Sometimes, however, we may need to transfer personal data to a recipient that is not a relevant authority in those terms. Before we can do this, we must meet all four of these additional conditions:

1. The transfer is strictly necessary in a specific case, for the performance of a task by the transferring controller, as provided by law for any of the law enforcement purposes.
2. The fundamental rights and freedoms of the data subject do not override the public interest concerning the transfer.
3. The transferring controller considers that the transfer to a relevant authority in the third country would be ineffective, or inappropriate.
4. The transferring controller sets out the specific purposes for which the data may be processed by the intended recipient and informs them of these.

What happens to subsequent transfers?

It is important that control of personal data is not lost once we have transferred it. It is vital that the rights and freedoms of individuals are still uppermost. Therefore, if the data we transferred is to be subsequently transferred elsewhere, it is important that those rights and freedoms continue to follow the data. For this reason, there are prescribed provisions that must be observed before any subsequent transfer can take place.