/* NO COMMENT */

EVERY POLICE STATION, EVERY DAY!

IMPACT ASSESSMENT

INFORMATION RISKS

Our business manages information risks in a structured way so that our management understands the business impact of personal data related risks and manages them effectively.

We have set out how we (and any of our data processors) manage information risk. We have a senior staff member with responsibility for managing information risks, coordinating procedures put in place to mitigate them and for logging and risk assessing information assets.

Where we have identified information risks, we have appropriate action plans in place to mitigate any risks that are not tolerated or permitted.

PROTECTION BY DESIGN

Our business has implemented appropriate technical and organisational measures to integrate data protection into our processing activities.

Under GDPR, we have a general obligation to implement appropriate technical and organisational measures to show that we have considered and integrated data protection into our processing activities. This is referred to as data protection by design and by default.

We have adopted and will implement internal policies and measures which help us comply with the data protection principles. This includes data minimisation, pseudonymisation and transparency measures.

DATA PROTECTION IMPACT ASSESSMENTS (DPIA)
Our business understands when we must conduct a DPIA and has processes in place to action this.

A Data Protection Impact Assessment (DPIA) has helped us identify the most effective way to comply with our data protection obligations and meet individuals' expectations of privacy.

An effective DPIA will allow us to identify and fix problems at an early stage, reducing the associated costs and damage to our reputation which might otherwise occur.

We must do a DPIA before we begin any type of processing which is "likely to result in a high risk". This means that although we have not yet assessed the actual level of risk we need to screen for factors that point to the potential for a widespread or serious impact on individuals.

In particular, the GDPR says we must do a DPIA if we plan to:

use systematic and extensive profiling with significant effects
process special category or criminal offence data on a large scale
systematically monitor publicly accessible places on a large scale

The ICO also requires we to do a DPIA if we plan to:

1. use new technologies
2. use profiling or special category data to decide on access to services
3. profile individuals on a large scale
4. process biometric data

5. process genetic data

6. match data or combine datasets from different sources

7. collect personal data from a source other than the individual without providing them with a privacy notice ('invisible processing')

8. track individuals' location or behaviour

9. profile children or target marketing or online services at them

10. process data that might endanger the individual's physical health or safety in the event of a security breach

We have also thought carefully about doing a DPIA for any other processing that is large scale, involves profiling or monitoring, decides on access to services or opportunities, or involves sensitive data or vulnerable individuals.

European guidance (WP248) provides a number of criteria that we can compare our intended processing against so see if a DPIA have be undertaken.

Even if there is no specific indication of likely high risk, it is good practice to do a DPIA for any major new project involving the use of personal data.

The DPIA have contain the following information:

1. a description of the nature, scope, context and purposes of the processing and ,where applicable, the legitimate interests pursued by our business;

2. an assessment of the necessity and proportionality of the processing in relation to the purpose;

3. an objective assessment of the risks to individuals, which considers both the likelihood and severity of the possible harm; and

4. what controls we have identified to address any of those risks, and whether those risks are eliminated, reduced or accepted as a result (including security).

If we have carried out a DPIA that identifies a high risk, and we cannot take any measures to reduce this risk, we need to consult the ICO. We 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.

FRAMEWORK

Our business has a DPIA framework which links to our existing risk management and project management processes.
A DPIA can address multiple processing operations that are similar in terms of the risks, provided adequate consideration is given to the specific nature, scope, context and purposes of the processing.
We have start to assess the situations where it will be necessary to conduct one:

1. Who will do it?
2. Who else needs to be involved?
3. Will the process be run centrally or locally?

If the processing is wholly or partly performed by a processor, then that processor must assist we in carrying out the DPIA. It may also be appropriate to seek the views of data subjects in certain circumstances.

DATA PROTECTION OFFICERS

Our business has nominated a data protection lead or Data Protection Officer (DPO).

That person takes responsibility for data protection compliance. We may need to appoint a DPO gong forward. Any business can appoint a DPO but we must do so if (and none of these apply) we:

1. are a public authority (except for courts acting in the judicial capacity);

2. carry out large scale regular and systematic monitoring of individuals (eg online behaviour tracking); or

3. carry out large scale processing of special categories of data or data relating to criminal convictions and offences.

We will consider designation of a DPO on a voluntary basis even when the GDPR does not require we to. The DPO will work independently, report to the highest management level and have adequate resources to enable our organisation to meet its GDPR obligations.

The DPO's minimum tasks are to:

1. inform and advise the organisation and its employees about their obligations to comply with the GDPR and other data protection laws;

2. monitor compliance with the GDPR and other data protection laws, including managing internal data protection activities, awareness raising and training of staff and conducting internal audits;

3. advise on and monitor data protection impact assessments;

4. act as the contact point for, and to cooperate with the ICO, and to consult on any data protection matter; and

5. be the contact point for individuals whose data is processed (employees, customers etc).

MANAGEMENT RESPONSIBILITY

Decision makers and key people in our business demonstrate support for data protection legislation and promote a positive culture of data protection compliance across the business.

We have made sure that decision makers and key people in our business are aware of the requirements under the GDPR. Decision makers and key people have lead by example, demonstrating accountability for compliance with the GDPR and promoting a positive culture, within our business, for data protection.

They have take the lead when assessing any impacts to our business and encourage a privacy by design approach. They have help to drive awareness amongst all staff regarding the importance of exercising good data protection practices.