Beacon meeting summary: Collection, storage, and use of data about domestic abuse and disclosures of domestic abuse

This is a summary of the key points discussed at an EIDA Beacon meeting, which was kindly hosted by EIDA Beacon, Collinson. Nicola Fulford, Partner at global law firm Hogan Lovells, explained the legal requirements when employers collect, store and use data about domestic abuse, including when an employee discloses their personal experience of domestic abuse.

This resource sets out what employers need to know to ensure responsible collection, storage and use of data to support victim-survivors of domestic abuse, as part of an effective workplace response.

Why collect data?

An organisation must be clear about why it is collecting personal data. There are good reasons to collect data about domestic abuse experienced by employees. Data may help an organisation to:

- Raise awareness within the organisation about the prevalence of domestic abuse.
- Provide better support to employees impacted by domestic abuse.
- Share experience and learnings with other employers to contribute to developing best practice.
- Gather evidence to support broader initiatives, including contributing to wider statistics or efforts to influence policy.
- Respond to requests to support police investigations or court proceedings in cases of domestic abuse involving one or more of the organisation's employees.

It is important for an organisation to measure the impact of its interventions to support employees impacted by domestic abuse, so that it can ensure those interventions are positive and effective. It is also important that this is done openly and transparently, without creating barriers to people seeking the information and support that they need.

Secure data collection and storage: General Data Protection Regulation (GDPR)

There are various categories of data subject to GDPR requirements, including:

- Personal data: information relating to an identified or identifiable natural person;
- Special category data: certain categories of personal data considered particularly sensitive (including data about a person's racial or ethnic origin, health, sexual orientation); and
- Data relating to criminal convictions and offences.

Information about domestic abuse may often include special category data or data relating to criminal convictions and offences, which are subject to stricter requirements under the GDPR. In cases where it is likely that this information will be collected you may be required to obtain the explicit consent of the individual. They must have a genuine option for

information about domestic abuse not to be stored or processed, whilst still being able to contribute to the initiative in question.

The data may be collected in a variety of ways. including:

- **Employee surveys** – These can be helpful to gain information about the prevalence of domestic abuse in an organisation and/or the support that employees want or find useful. Employee surveys will fall outside GDPR requirements if they are anonymous, and the employee cannot be identified by the information given in response.
- **Discussion groups** – These can help an organisation to gain an in-depth understanding of employees' experiences of domestic abuse and the usefulness of the support offered by the organisation. Written notes or recordings of such meetings are likely to contain sensitive personal data. Thus, those taking part should agree that the discussions are confidential. They should also be told how the discussions will be recording and whether the recording or any summary will be shared with others.
- **Employee disclosures** – An employee may disclose information about domestic abuse to their employer voluntarily, for example if they are seeking support. The employee should be reassured that the disclosure is confidential. The employer should take a record of the conversation as the employer may be called on to provide evidence in an investigation by the police and in court proceedings. The information should only be disclosed to others if it is necessary to provide help and support and with the prior consent of the person who has made the disclosure. The only exception to this is if the person to whom the disclosure is made considers there to be an imminent threat to life, harm to children or threat to the employer, in which case the employer should contact the police as soon as possible.

The transparency principle under GDPR requires those collecting data to provide data subjects with clear information about how and why data is stored. An overview of what information is required to be provided can be found in articles 13 and 14 of the GDPR.

Good practice:

- Electronic storage of any sensitive information must be secure, meaning a password-protected folder (or similar), with restricted administrative access and not local storage on an individual computer. Multi-factor authentication for logins is recommended.
- While access is restricted, relevant individuals such as the HR manager should have access as needed. Share information on a "need to know only" basis. Ensure that those who collect data are properly trained.
- It is important to have a policy or guidance that covers disclosures of domestic abuse so relevant individuals (HR, Domestic Abuse Champions, Saferguarding Officers etc) are properly informed about secure data collection and storage.
- Data may be stored for "as long as necessary". If an individual leaves the organisation, they should be reminded of their stored personal data and asked whether they wish for it to be kept or deleted.

If you are unsure or have concerns about data collection and storage, Data Protection Impact Assessments (a process for identifying and minimise data protection risks) can provide useful ways of mitigating these.

Dealing with law enforcement: Duties of the employer

You can ask for the employee's consent to share information with the police. Do not share information *proactively* with law enforcement unless you have the explicit consent of the individual or there is a safeguarding risk if you do not share it.

You may receive a request from the police to provide information. If this happens, take steps to ensure that the request is indeed from the police, and not someone pretending to be the police in order to access the data. If the police have a warrant, you are required to share the information with them.

You may also be approached by a third party (including the perpetrator) with a Data Subject Access Request (DSAR). The deadline for responding to such requests is one month. In responding to a DSAR, it is important to note that you are within your rights to exclude information that may put the victim-survivor at risk. Safeguarding has priority over data-sharing.

Safeguarding is key

Someone may make a disclosure about themselves or a third party. Inform whoever makes the disclosure that while the information is confidential, you have a duty of care to breach the confidentiality if there is a risk to safety. This is called a "vital interest" reason to share sensitive information with the police or other services.

[June] 2024