Risk assessment and risk management by police

Step 6: Develop procedures for information management and confidentiality

Information management and confidentiality should be based on agreements (formal protocols or any other form that is considered appropriate at national/local level) developed for the timely and appropriate sharing of information between the police and other agencies. These should:

- be drafted in close consultation with the national data protection authorities (105) to ensure compliance with the GDPR and national legislation;
- clearly define the range of information that can be shared and with whom;
- determine when the duty of confidentiality might have to be breached (e.g. when a victim is at serious risk), in accordance with national legislation;
- distinguish between situations that involve only adults and those where children are also involved, in accordance with national legislation;
- be known to and understood by professionals, and communicated clearly to victims and perpetrators;
- be reinforced through multiagency training of relevant professionals (on implementing systematic police training and capacity development, see Step 4; on embedding police risk assessment in a multiagency framework, see Step 5).

The sharing and transferring of information between the police and other agencies and services is a key aspect of risk assessment of intimate partner violence (see Principle 2 on risk assessment). The failure to share information on risk can lead to failings in the system that put women and children at increased risk of further harm. All appropriate and available resources should inform the assessment of risk, including the victim, the perpetrator, case history files and information from other agencies.

However, risk assessment must be conducted in a way that protects a woman's privacy, guarantees confidentiality and discloses information only with her informed consent. Sharing information about a woman's experience of violence inappropriately can have serious and potentially life-threatening consequences for her and her children (see Principle 5 on risk assessment). The police should have well-developed and clear information on sharing agreements with partner agencies in a multiagency framework (see Step 5), defining what information should be shared, on what basis and with whom.

Confidentiality and data protection are often barriers to the sharing of information among stakeholders in a multiagency system. A current challenge for the police and other sectors across Europe is the implementation of the general data protection regulation (GDPR) (104). Information- and data-sharing regulations can support or prevent timely and appropriate policing and multiagency working. Police leadership should consider negotiating relevant provisions for information sharing with national commissioners for data protection, with the aim of improving public protection and community responses to intimate partner violence against women.

It is essential that clear protocols and/or methods for information sharing, both within and between agencies, about women at risk of, experiencing or perpetrating intimate partner violence are developed and implemented in accordance with national legislation. With the support of national data protection commissioners, these can provide clear guidelines for timely and appropriate sharing of information among agencies that comply with national and EU regulations, and protect the privacy and well-being of victims and their children.