Victim Support Europe

With financial support from the Justice Programme of the European Union

VICTIM SUPPORT AND DATA PROTECTION

some concerns and proposed solutions for victim supporters

Contents

Introduction

Victim support has been a vital and necessary service in every society for decades. The core nature of victim services has been accentuated in recent months, with the outbreak of COVID-19, when a number of countries has declared victim support as an essential service – one that needs to continue even as the vast majority of social and economic activities are put on hold[1]. Indeed, the European Commission in its recent EU Victims Strategy has also recognised the essential nature of victim support services.

At the core of quality support services is the flexible response to the individual needs of victims - supporting the victim and their loved ones while doing no harm to either the victim, their loved ones or any third person. For this reason, victim support organisations naturally follow strict ethical principles and aim to deliver an elevated standard of services to victims, which incorporates confidentiality as a foundation of providing services to victims.

Arguably, long before the establishment of extensive data protection standards, victim support workers and organisations were at the forefront of protecting victim information and confidentiality. Indeed, confidentiality has been a foundational standard for VSE and its members since its inception, 30 years ago.

For decades, victim support professionals have been ensuring victims' privacy almost intuitively. They have advocated for services to be confidential and promoted this position in EU legislation on victims' rights. They have implemented data privacy in accordance with EU and domestic legislation, with great care and at a significant cost and investment.

This has often meant that victim supporters had to balance the necessity to collect and store victims' data in a sensitive and sensible manner while also ensuring data sharing in an ethical and efficient manner. They have done it through different approaches. Some organisations decided to only store sensitive victims' data in a single paper copy, kept locked in a safe. Others opted for storing data in a single computer, which remained off-grid. In certain situations, victim support organisations have gone as far as to not seek, collect, store or process any personal data from victims they support.

Basically – victim support organisations have been doing their best to build and maintain a relationship of trust with victims and make sure the victims they serve feel safe.

Victim Support Europe has long recognised this important aspect of victim services. In our 2012 publication: Statement of Victims' Right to Standards of Service[2] – we set out confidentiality standards that ensure members were committed to:

- Holding in confidence information given to them by or about a victim - accordingly no member should disclose to any third party information received from or relating to a victim unless:

[1] VSE has advocated for victim support services to be officially recognised as essential services. This has been recognised by the European Commission, which recommended this approach to all the Member States in the EU Strategy on victims' rights 2020-2025. See https://ec.europa.eu/transparency/regdoc/rep/1/2020/EN/COM-2020-258-F1-EN-MAIN-PART-1.PDF

[2] https://victimsupport.eu/activeapp/wp-content/files_mf/1348589602service_standard_rights.pdf

(a) the victim has consented, or
(b) there is a legal requirement to do so, or
(c) there is an overriding moral consideration

- having clear procedures for dealing with such situations
- having a public complaints procedure for dealing with alleged breaches and any other complaints.

We have continued to promote the necessity for protection of victims' data through our Standards and Accreditation system, which placed on our (full) members the onus of ensuring victims' safety and confidentiality of victim support services.

The introduction of new rules under EU GDPR – 2018

Whilst victim support approaches to data protection took place within the backdrop of EU data protection rules that have been in place since 1995, the coming into force of the General Data Protection Regulation (the GDPR) in 2018, has had a significant impact on support organisations.

For a number, the situation has been close to overwhelming, with rules that should enhance victim safety sometimes putting at risk the very operations of the organisations that help them. The unintended risk of the GDPR is that data protection in victim support stops being driven by the inherent concern for victims' well-being and becomes a desperate attempt to conform with rules and avoid large scale fines.

To add to the complexity of the already sensitive situation, these rules are deliberately left vague. To understand how best to apply them requires significant external or in-house expertise at significant cost.

Yet, even when a significant investment into GDPR compliance is made, organisations are still exposed to different interpretations of national data protection authorities due to vague rules. This exposes even the most careful organisations to the risk of repercussions indicating that that current system too often fails to respect the reality of victim support services.

What originated as legislation driven by (mis)behaviours of large profit making businesses and the expansion of the internet is now applied horizontally and equally to everyone. This has created challenges for victim support organisations where issues such as capacity, the importance of their mission or, of their ability to endure financial penalties for unintended mistakes are not fully understood or taken into account.

Large international businesses can afford to build into their business model the risk of being fined for GDPR violations and even take calculated risks to generate larger profits at the expense of potential data protection violations[3].

[3] For example, in 2019 Google Inc was fined with € 50 million by CNIL – the French data protection authority, for breaches of GDPR – the highest GDPR breach fine to date. See more at: https://www.cnil.fr/en/cnils-restricted-committee-imposes-financial-penalty-50-million-euros-against-google-llc

On the other hand, a small organisation providing essential services usually cannot afford even the smallest mistake as even a relatively small fine might mean the end of their existence and the interruption in lifeline services to vulnerable victims.

It is critical for victim support services that data protection is balanced with multiple general and fundamental rights such as right to privacy, right to life and right to justice – all three of which victim support organisations protect.

This is not to say that the GDPR has not benefited the privacy of victims. All organisations, including support organisations, should have clear a clear legal framework which ensures they properly protect victims' data.

Every victim support provider needs to have clear and transparent policies about how they collect, store and share victims' data. These policies need to ensure that
- data is stored safely and responsibly
- access to sensitive victims' data is given only to a limited number of specifically authorised personnel
- those accessing data are trained in how to deal with data safely
- those accessing data are held responsible for any potential breeches of victims' privacy

The concern brought to VSE by support organisations is that the framework is far from clear. GDPR has introduced broad and vague rules, which are interpreted by 27 national data protection authorities – which do not necessarily have to share the view of the fine details of its application. In effect, organisations have to operate to different rules or approaches.

This can seriously undermine legal certainty. Namely, GDPR starts from the premise that all data controllers are accepting a certain level of risk in collecting and processing personal data. With such vague rules in place, and the understanding that it is impossible to fully protect personal data, instead of the authorities having to prove a failure to comply, it appears as GDPR effectively requires organisations to complete the impossible task of disproving a negative notion – that they have not not-complied with GDPR.

Ultimately, there is concern that the framework inhibits the ability of organisations to efficiently serve victims and that objectives of data protection could be achieved in a more proportionate, consistent and co-ordinated manner.

Numerous discussions have taken place within VSE and amongst our membership on how to ensure compliance with strict and sometimes quite demanding formalities and provide best support to victims in need. In some organisations, this raised a number of questions and required changes in how victims' data is collected, stored, and shared.

This paper aims to help our members navigate safely through GDPR while ensuring the best services for victims they support. It also aims to initiate a discussion at the European level on the operation of the GDPR from the perspective of civil society service providers, to explore

problems arising from the implementation and interpretation of the GDPR and to examine possible European and national solutions.

GDPR Glossary

GDPR introduced some specific language, which has specific meanings as regards data collection. This is the interpretation of some specific terminology as it applies to the provision of victim support.

Data subject – is the individual, a living physical person, whose data is subject to protection. Data subjects can be victims, their family members or, in cases of human resources issues, also victim support workers.

In the language of GDPR, victim support organisations are either **data controllers or data processors** (or both).

When an organisation decides what type of data to collect and for what purpose, they act as data controllers. Organisations will then usually also process the data themselves, but they can also entrust some or all of the data to an external party for processing.

Processing is any action of using the personal data for an end purpose – e.g. to send victims' reminders for appointments, inform them about an upcoming trial or have them participate in an information campaign. When processing is entrusted to an external organisation, victim support organisations need to describe precisely and in a limited manner for what purpose data is shared and ensure that data is only used for that particular purpose. It is recommended to enter into a particular agreement with the data processor for that purpose.

Example 1: if a victim is murdered, collecting their own personal data is not regulated by GDPR. However, identifying the victim can also lead to identification of their family members or their neighbours and can expose their own privacy. Therefore, it can lead to identification of living persons, whose data is subject to GDPR protection.

Example 2: if a crime happens within a business environment, data related to legal entities can be freely collected, from the GDPR perspective. However, if it can lead to identification of employees or owners of the business, GDPR applies to that type of data.

It is important to remember that GDPR is only applicable to digitalised data – hence, data stored in a digital form – an excel sheet, database, case-management system or other digital or electronic format – in a computer, USB stick, smartphone or other digital storage. Asking the victim for their name and other personal details, during intake, is not subject to GDPR as long as it is not stored in a digital form, even if it is kept on the paper. It might, however, be subject to other forms of limitations, depending on specific national legislation.

This means that, as long as an organisation does not store victims' personal data in a digital way which can lead to their identification, GDPR is not applicable.

Example: Organisation A is storing victims' files in a paper file, but still keep anonymised metadata for statistical purposes – e.g. number of victims, type of crimes, type of services provided, gender, language of victims etc. Organisation A is not a data controller or processor, from the perspective of GDPR, given that the digital data is not personal data and personal data that is kept in paper file is not subject to GDPR.

Applying EU data protection rules in victim support services

The main feature of GDPR protection is its focus on individuals' right to control their own personal data and the obligation that the entity controlling and processing the data has a legal basis for doing so. Two fundamental questions need to be answered when determining if the GDPR applies in an individual victim support situation and whether data under GDPR can be processed.

- Firstly, the data needs to be considered personal as defined by the GDPR.
- Secondly, an organisation needs to have a legal basis to control and process such data.

Defining Personal Data

The GDPR considers personal data very broadly, as **any information relating to an identified or identifiable natural person.** To determine if information is personal:

- The information must relate to an individual; and
- The individual can be identified based on the information.

According to Article 4(1) of the GDPR, these personal identifiers include the name or other factors specific to the economic, cultural or social identity of that natural person. As such, there may be information about a person which doesn't fall under GDPR where there is no identifying information such as name, date of birth, phone number or address to connect the information to the person.

This means that **collection of anonymised data for statistical purposes,** such as a victim's gender, age or type of crime, **will normally not be considered as data falling into the category of protected information** for the purposes of GDPR, as long as it is collected in such a way not to result in the victim's identification.

Yet, knowing this basic information, doesn't always enable a support organisation to know if they fall under GDPR in a given case. Below are some examples of different scenarios.

Victim Support Example

A young man calls a victim support helpline seeking assistance. The support worker takes information on the crime and the needs of the victim. The victim states that he would like to arrange a meeting with a local victim support office.

Case 1
The helpline worker takes the first name, email address and telephone number of the victim and inputs this into the organisation's case management system.

The information is then provided to the local victim support office (part of the same organisation) so they can contact the victim to arrange an appointment.

Question: Does the GDRP apply in this situation?
Answer: Yes – GDPR applies, since the victim is clearly identifiable from the data collected.

Case 2
The helpline worker, records some basic details of the crime (e.g. that it concerned sexual abuse or online fraud) and needs of the victim; however, not recording their name, phone number or e-mail address. In the case management system, they note that the victim would like an appointment.

They provide the victim with contact information for the local branch and ask them to call or email directly.

In the case management system, the case is assigned a reference number and the information made available to the local branch in the event the victim calls. The victim is provided with the same reference number for when they call.

Question: Does the GDRP apply?
Answer: No, GDPR does not apply, as it is not possible to infer their identity from the data collected.

Case 3
The same facts apply as with Case 2. However, in addition to crime and needs information, the helpline worker also includes information that the victim is a Muslim, LGBTI victim of hate crime?

Question: does the GDRP apply?
Answer: It depends on whether it is possible to backtrack the victim's identity from the data collected. If it concerns a hate crime against a Muslim LGBTI victim, that was well covered by the media, it might indeed be possible to identify them even if no personal data is taken. If there is no possibility to do so, the GDPR would not apply.[4]

For personal data which enables a victim to be identified, the victim support organisation needs to always have a **legal basis to collect, store and process personal information**.

[4] However, when sensitive personal data is collected (such as religion, sexual orientation, gender identity), some other rules may also apply, so it might still affect the data collection process.

Legal Basis for Collecting Data

GDPR is aimed at regulating the collection of personal data and provides several legal bases for their collection. **Consent is often relied on as the main legal basis but is only one of several of the possible legal grounds for processing of personal data under the GDPR.**

Notably consent can be more complicated to obtain in the victim support context, and may not be necessary. Exploring alternative legal bases for processing data can improve the victim experience and help organisations maintain efficient processes.

The most appropriate basis to use will depend on the relationship of the data controller with the data subject. Responses from Victim Support organisations also indicate that it depends on national interpretations and approaches of Data Protection Commissioners.

Article 6 GDPR provides for different bases for lawful processing. What are the legal bases for lawful data processing?

- **Consent** – the individual has given clear, unambiguous and fully informed consent for the controller to process their personal data for a specific purpose;
- **Contract** – the processing is necessary for the performance of a contract an organisation has with the individual, or because they have asked the organisation to take specific steps prior entering into a contract;
- **Legal obligation** – the processing is necessary to comply with a legal obligation to which the organisation is subject;
- **Vital interests** – for example, the processing is necessary to protect someone's life;
- Performance of a task carried out in the **public interest** or in the exercise of official authority – the task or the authority must have clear basis in law;
- **Legitimate interests** – the processing is necessary for the organisation's legitimate interests or the legitimate interests of a third party unless there is a good reason, such as the protection of fundamental rights and freedoms, to protect the individual's personal data which overrides those legitimate interests.

Any of the above bases is equally acceptable, from the GDPR perspective - none of them takes precedence over the others. However, some forms of bases are more practical and less burdensome for both victim and victim support organisation.

What is important to assert, however, is that:

- There may be more than one legal basis to collect and process data, but one is enough;
- There is no hierarchy of legal basis – all are equally valid;
- There is no blanket authorisation to process data under any basis – each individual instance of data collection and processing needs to be justified on its own merit;
- Organisations need to be able to present, at request, all data collected in relation to any data subject;
- Organisations need to be able to disclose any instance of data processing in relation to each data subject whose data they collected;
- It is up to the organisations to ensure that their data collection and processing practices are not only GDPR compliant, but also ethical.

Consent

This is the most often mentioned, and sometimes referred to as the 'default' basis for data collection. However, it may be one of the most complicated bases, in the context of victim support. To be acceptable for the purposes of GDPR, the following rules apply:

1) Consent must be:
a) Clear
b) Unambiguous
c) Fully informed
d) Recorded so that the victim support organisation is able to demonstrate that a victim has consented to processing of his or her personal data

2) The request for consent must be presented in a manner that is distinguishable from other matters to which consent may be given as well, and it must be gathered in a manner which will identify all purposes for which data is collected (e.g. if data is collected for case-management purposes, it cannot then be used for referral or for individual assessment).

3) If a victim does not want to share their personal data and they are told the provision of services is only possible if they provide it, consent cannot be considered to have been freely given. In such a situation, legal basis for data processing should be found elsewhere – e.g. in legitimate interest.

4) A mechanism needs to be created by which a victim may easily withdraw his or her consent.

In practice, to fully and genuinely comply with these requirements, the victim support worker will need to talk through a range of legal and formal issues before registering a victim's name or any other personal data.

The support worker needs to explain to a sufficient amount of detail to the victim, what type of data will be collected, for what purpose, what is the procedure for withdrawing consent and then have the victim sign a release form. In case the support is provided on the phone, or if the victim has any difficulties in signing the form (illiteracy, disability etc.) the consent can be given orally and case-worker can take it down in writing, while explaining the circumstances.

Taken against the reality of providing victim support, in particular as a part of **first response or first contact with the victim**, when victims are likely to be more highly traumatised and their cognitive abilities likely affected by the crime, it becomes obvious that this formalistic approach is likely to be counterproductive. In the case of the operation of helplines, it can be even more complex.

"When a victim calls in, the last thing they want is a complicated reading of their data protection rights. We have to allow them to speak and we need to listen in a caring manner. Finding the right way to obtain consent to record information in this situation is really tricky and I'm worried it will put victims off"

Victim Support Worker

This is additionally complicated by the fact that often the victim support organisations of first contact will not be able to provide full support to victims and referral will be required.

Case study:

*A highly traumatised victim of sexual assault, contacts a 116006 helpline to seek support. The assault happened a few hours ago and she has not reported the crime and has not yet told anyone about the incident. The 116 helpline is run by Organisation A. The helpline worker asks the victim for her name during conversation, to be able to establish a personal connection, writes the name down on a piece of paper (**data collection point 1** –GDPR not applicable, because the name is only written on the paper) which will be destroyed as soon as the call is over. The helpline worker also collects other anonymous data (gender, age, date of the incident, gender and age of the alleged offender, previous victimisation etc.) and enters it into the database of Organisation A, for statistical and reporting purposes (**data collection point 2** – GDPR not applicable, because data is anonymised).*

*The helpline worker tells the victim about the psychological support service that Organisation B is running. The victim decides she wants to talk to the psychologist. She gives her phone number to the helpline worker to have the psychologist call her back. The helpline worker sends the victim's name and phone number by e-mail to the psychologist with the message to call as soon as possible (**data collection point 3** – GDPR applicable, yes, because the name and phone number are written in an e-mail).*

*The psychologist calls the victim back after ten minutes. During the consultation with the psychologist, the victim reveals more details about her crime that the psychologist registers into Organisation B's case-management system. This includes the victim's name, phone number and some details about the circumstances of the crime (**data collection point 4** – GDPR applicable, because personal data is entered into the Org B's case-management system).*

*During the conversation with the psychologist, the victim also decides to have a rape kit collected by forensic specialists and to report the assault to the police. The psychologist sets up an urgent forensic appointment at the specialised centre, run by Organisation C. The specialised centre is in the same building as the psychologists' office, so he just walks there. He dictates the victim's name and contact details and some details regarding the circumstances of the crime to the receptionist who enters them into their internal case-management system (**data collection point 5** – GDPR applicable, because personal data is entered into Org C's case-management system).*

The Victim arrives at Organisation C for forensic examination two hours after her first call to the helpline.

At each point where GDPR is applicable, legal basis for data processing needs to be determined and recorded appropriately. Each organisation needs to be able to show

Based on the above case-study, the victim's data is controlled and/or processed in at least five points and at least three of these, the data controller and/or processor need to make sure that they have legal basis for data processing. It is unrealistic to expect that in the span of one hour victim's consent is sought three times, with all the detail and scrutiny GDPR sets on the consent to be considered valid.

This will mean that at the intake point, victim support organisations cannot fully anticipate what will be further requirements for referral and solicit full consent before the totality of victims' needs is known. Such anticipation will rarely be possible before an individual assessment is conducted.

Taking the victim through several instances of the provision of the same information through the same formalistic approach, especially with highly traumatised victims, is likely to cause secondary victimisation.

Not only is the approach not always ideal from a victim perspective, there are administrative burdens to be considered. Victim Support organisations, particularly NGOs already face a range of financial difficulties and often have waiting lists for victims. The additional burden of lengthy consent processes when accumulated over large numbers of victims could simply mean that fewer victims will be able to receive services. This is particularly the case where organisations have not received additional funding to cover the costs of implementing data protection rules.

It is obvious, therefore, that consent is often far from the ideal basis for data processing in the context of victim support.

Case study:

A highly traumatised victim of domestic violence calls a 116006 helpline to seek advice on how to protect herself and her small children.

To fully provide the information, the helpline worker needs to collect some of her personal data, including name, address, phone number, children's ages and names, and details about her employment, family life and social networks.

Before asking any of these questions, the helpline worker is given a script that she needs to read to the victim, to ensure that the victim understands the GDPR implications of data processing and to be able to give informed consent. The script is about 2 pages long, is very technical and takes about five minutes to complete. Several times during the reading of the

script, the helpline worker needs to insist that the victim repeats certain statements, to ensure that the consent was freely given.

Four minutes into the call, the victim hangs up as her abusive partner came back home. She decides that she will never call the helpline again.

Contract as a legal basis for data processing

Some victim support organisations may have a practice of entering into a contract to define the type and scope of services which are provided to the victim. Some particular professions, such as psychologists, can have it as a standard practice. If that is the case, such a contract can serve as a basis for data processing, as long as data is collected and used towards the execution of the contract.

Depending on the circumstances, it may be argued that even where there is no document titled 'contract on providing victim support services' the provider and client are entering into a type of a contractual relationship. For example, when buying a product online means that we entered into a contract, and to execute the contract, the seller needs our personal data, which they can ask for under this legal basis.

The same may be argued for some types of victim support services. If a victim calls and asks for a support worker to accompany them to a trial, it is reasonable to require their name and some details about the trial (the time, date, specific location), to know where and when to send the support worker.

In this regard, contract, much as consent, needs to be an expression of free will and an informed decision by the victim.

Legal obligation

A legal obligation to provide a certain service may be a basis for data collection and processing, if such data is essential to comply with the legal obligation. For example, this may be the case with the implementation of court orders, supporting vulnerable victims, such as children or when support organisations implement a duty established in law. Similarly, a financial institution may be legally obliged to process personal data of victims of banking fraud and will hence have a legal obligation justification to process data.

To claim the legal obligation, the specific organisation has to established that it has a specific obligation in relation to a specific victim. General statements cannot be used as justification. However, this basis cannot be exercised if the support organisation has a discretion on whether to process personal data or if there is another reasonable way to comply.

Vital interest

Some elements of victim support might be considered as acting to protect victims' vital interests, in particular in cases where the lives or health of victims themselves or other persons are at stake. For example, taking contact details of a highly traumatised victim to

follow up on their wellbeing after a week, even if they might refuse support in the immediate aftermath.

Notably, evidence suggests that many victims of terrorism who have not suffered serious physical injuries will refuse support in the first instance. However, after the first shock has worn off, they may feel the impact and seek out support. Taking this into account, arguably it would be in vital interest of the victims to keep their phone number and carry out follow up calls in the subsequent days or weeks.

Legitimate Interest

Victim support organisations may rely on **legitimate interest** when there is a clear benefit to a data subject (victim) and to the organisation resulting from the data processing; in other words, when there is a compelling justification for the processing.

The legitimate interest basis is the most flexible of the legal bases provided by the GDPR. It may be useful to rely on the legitimate interest when it is difficult to obtain consent from data subjects and where the impact of data processing on victims' privacy and data protection rights is minimal.

Legitimate interest cannot be a blanket legal basis for each data processing instance - GDPR insists that it needs to be based on the individual circumstances. However, this does not mean that victim support workers need to go into detailed data processing impact assessment each time they collect personal data.

To apply legitimate interest, it is recommended to conduct a three step test:

- **Purpose test** – is there a legitimate interest behind processing? Arguably, the organisation has a legitimate interest to support victims of crimes based on the Victims' Rights Directive and applicable domestic legislation.
- **Necessity test** – is the processing necessary for that purpose. Normally yes, as we need to understand who the victim is and what they have gone through to be able to support them appropriately. We need to collect and process their data to be able to help them.
- **Balancing test** – is legitimate interest overridden by the individual's interests, rights and freedoms? This would rarely be the case, as the processing is in the individual's interests and to ensure their rights and freedoms are implemented.

It is however necessary to explain clearly the purpose of the processing and to demonstrate the necessity of the processing to data subjects. For that reason, a victim support organisation must perform a balancing test that would give proper justification to interests and fundamental rights and freedoms of data subjects.

Given the mission and activities of victim support organisations, this should not be a difficult exercise. Nevertheless, it is important to pay attention to these processes, justifications and reasoning so that relying on the legitimate interest basis is GDPR-compliant.

Case study 1

A young man who calls a victim helpline explains his situation (subject to a violent attack – possibly hate motivated) and agrees that he would like an appointment for further help.

In order for an appointment to be made, Organisation A records personal data including name and contact information of the victim, details of the crime and what requests he has made. This information is provided to a local branch which contacts the victim to book an appointment.

In this instance, legitimate interest is used as a legal basis for processing. However, it would be a good practice to inform the victim in some detail how their data will be processed and used and to let them know how they can request their data to be removed. They are also told about where to find the organisation's full data protection policy for more information.

Case study 2

A young man who calls a victim helpline explains his situation. He wants some basic information on his rights but does not want to make an appointment. The VSO took some initial personal information to facilitate their helpline support.

However, the VSO has a policy to recontact victims of violence (as in this case) after 1 week to check if the victim is ok and if they would like any further assistance. All information on the case is retained to enable to follow up contact.

Question: Is there a legitimate interest for processing the data? Does the organisation need to obtain consent in order to retain, process and recontact the victim?

Answer: Yes, it may be justified that legitimate interest exists to retain data and call the victim back up, but it will also depend on the circumstances of the case. Violent crimes can easily justify legitimate interest, but it can also be claimed when victims are vulnerable, or when other circumstances can justify the need to retain victims' data for a certain period of time. The case worker would need to make an assessment as to whether it is justified or not, and make an affirmative declaration to that effect in the case-file in each individual case. This exercise does not have to be too complicated and can consist of multiple choice questions for the case-worker to respond to, but needs to provide sufficient base to retain and process data.

It would, however, be a good practice, to inform the victim about the possibility of the call next week and to give him an opportunity to refuse the follow-up. As above, further good practice would inform the victim about data retention and deletion principles and tell them where to look for the full data protection policy.

Public interest

If a victim support organisation is entrusted with a task performed in the **public interest** or with the exercise of official authority that would have a clear basis in law and would implicate processing data of victims or other persons, it may use this as a legal basis for lawful data processing[5]. For this to be the case, the particular data controller (victim support organisation) needs to be affirmatively declared to be performing the public interest task.

Providing some element of support, assistance and services to victims of crime may be considered tasks performed in the public interest. The relevant recital (41) GDPR clarifies that this does not have to be an explicit statutory provision as long as the application of the law is clear and foreseeable. However, the safest and clearest way is that either the organisation or the delivery of support, assistance and services to victims of crime is described in national law as public interest tasks.

This legal basis for lawful data processing therefore strongly depends on the applicable national laws and, in the absence of their clarity, their interpretation by the national data protection authority.

Some elements of victim support, in particular if data is processed to ensure wellbeing of vulnerable victims or to ensure public safety, can be justified by public interest.

Example

In the Netherlands, the Minister of Justice issued a ministerial regulation, appointing Slachtofferhulp Nederland as the coordinating legal entity for the support of victims of crime in the Netherlands. Driven by this regulation and its wording, Slachtofferhulp is considered to be acting in the public interest when they provide support to victims of crime. This is additionally reaffirmed by the fact that victims of violent crimes in the Netherlands are automatically referred to the support services by the police. Through this referral some of the victims' personal data (name, phone number, address) is transferred to support services by the police – arguably in their exercise of public interest activity when they work on responding to a report of a crime.

Slachtofferhulp Nederland also supports victims of traffic accidents. These victims are not mentioned in the ministerial regulation or in a law, which means that the public interest basis is more difficult to justify. As a result other legal bases are used, usually consent.

The argument that victim support services in Europe are of public interest has been reinforced in recent months. From a practical perspective, victim support organisations have been critical to social functioning in the wake of the Covid-19 pandemic. At the national and international level, there have been regular demands that support services remain open, that

[5] It is also important to note that if data processing is based on the legitimate interest, the public task or authority basis, the data subject should have the right to object to data processing on grounds relating to his or her particular situation in accordance with Article 21 GDPR.

they receive additional funding to cope with Covid-19 related crime issues and that in order for them to continue operating under lockdown restrictions, they be recognised as essential services. This approach was indeed adopted in several countries.

Additionally, the European Commission itself has recognised the important position of victim support organisations and called on Member States to recognise them as essential.[6] This move was important in view of the increase in certain types of crimes, in particular domestic violence and the increased need for support services for victims.

Safely storing victims' data

In addition to the question of whether data is personal and whether there is a legal basis for processing it, any victims' personal data must be stored correctly.

There are two main approaches to data storage: on paper and digitally. Personal data that is recorded on paper – forms, documents, medical files etc., should always be stored in locked rooms or cabinets. While GDPR does not apply to such data processing, it should always be considered as a good practice to have a set of safeguards regarding who can access paper databases and under what conditions.

Regarding digital data, it must be protected and organisations must be able to show they took reasonable measures to secure the data. This may be through e.g. password protection for limiting access or some other system which ensures that only those who have a justified interest to access data will have the possibility to do so. However, data protection professionals suggest that sensitive personal data of victims should always be encrypted[7]. In this regard, there are three main approaches:

If service providers opt for **local, on-premises storage of encrypted data**, it will be encrypted and stored locally on servers kept inside the organisation. Hardware for servers will be required, the servers should be kept in a space with limited access – usually a locked server room, and organisations need to budget for maintenance of the server by professionals.

Alternatively, data can be kept in **cloud storage with server-side and in-transit encryption.** Here, a trusted cloud provider must be identified which encrypts client data and stores this encrypted data as well as the corresponding encryption and decryption key in a secure place.

In that case, the provider can decrypt data on the request of an authorised person. Such services are offered by almost all cloud providers like Google, Dropbox, Microsoft, Amazon, etc.

[6] EU Strategy on victims' rights (2020-2025): https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52020DC0258&from=EN

[7] For more information about encryption, see e.g. https://www.internetsociety.org/encryption/what-is-encryption/?gclid=EAIaIQobChMIj8r86NK_6gIVFOh3Ch2Q4wwBEAAYASAAEgIl6_D_BwE

From the experts' perspective, the safest way to store sensitive personal data is through **cloud storage with client-side, end-to-end encryption.** In this case, the service provider encrypts the client data on their side and stores the encrypted data in the cloud. This way, the service providers are the only ones who can access the decryption key and no one else, not even the cloud provider can. This type of encryption is offered only by some vendors (for example MicroSoft[8]). The particular benefit of this type of encryption is that even if the provider is asked by the authorities to access the victim data – they cannot do it as they do not have the encryption key.

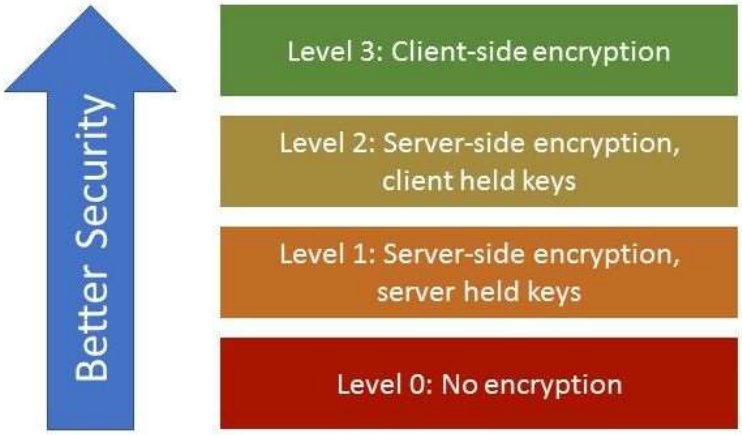


Image: Safety ranking of encryption options[9].

To estimate the best solution for data storing, victim support organisations should conduct a risk assessment exercise and decide what level of protection to go for. The saying is that there is no 100% safe way to store data, but some approaches are riskier than some others.

While in depth analysis of these risks falls beyond the purposes of the present paper, the following risk matrix may be used as a starting point in identifying necessity for managing certain risks more vigilantly than some others[10]:

8 https://azure.microsoft.com/en-us/services/azure-dedicated-hsm/
9 Image credit of: https://www.eenewseurope.com/design-center/client-side-vs-server-side-encryption-who-holds-key/page/0/1
10 Image credit of: Deloitte Privacy Knowledge Center, Data Protection Officer Course, October 2020

Controls	Physical	Administrative	Technical
Preventive	• Physical security perimeter (6.8.1.1) • Physical entry controls (6.8.1.2)	• Information security awareness, education and training (6.4.2.2) • Policies and procedures • Notices (7.3.2) • Engaging of a subcontractor to process personal data (8.5.7) • Contact with authorities (6.3.1.3)	• Information backup (6.9.3.1) • Management of privileged access rights (6.6.2.3) • Intrusion Prevention Software (IPS) • Segregation of duties • **Cryptographic controls (6.7.1)**
Detective	• Securing offices, rooms and facilities (6.8.1.3)	• Internal audit (5.7.2) • Third party audit (e.g. 8.5.3)	• Protection from malware (6.9.2) • Logging and monitoring (6.9.4)
Corrective	• Protection against external and environmental threats (6.8.1.4)	• Breach notification (8.5.4) • Reporting information security events (6.13.1.2)	• Segregation in networks (6.10.1.3)

Having said this, ultimately, EU rules still leave organisations in a situation of uncertainty. Unless they carry out the absolute maximum, rather than what they perceive to be reasonable, there is no guarantee that it will be accepted. This is particularly difficult for NGOs which have very limited resources and which seek to maximise those resources for the core tasks of supporting victims.

Data processing by victim support organisations

Data processing by victim support organisations should, as discussed previously, be guided by not only GDPR, but also the requirements of confidentiality of services and respectful treatment of victims.

This means that a victim support organisation should ensure that:

- Only data that is necessary to provide a high quality of service is collected;
- Only support professionals and other staff in the organisation who need to have access to personal data to support a victim or perform their professional duty have such access;
- Any access to data is allowed only when necessary and each instance of access to data is recorded;
- Data is processed and shared (both internally and externally) only to the extent absolutely necessary to ensure the best support for the victim or to comply with statutory obligations (e.g. for auditing purposes);
- Data is stored during the time the victim is actively receiving support from the organisation and for a determined period of time after closure of their file – but not longer than 5 years after the file is closed;
- Data is deleted after the expiry of the above period, or as soon as victim has requested that data is removed.

Personal data can be anonymised by support organisations and kept as such for an indefinite period of time, for statistical and reporting purposes.

Rights of Victims as Data Subjects

Victims have certain rights in their capacity as 'data subjects'. Some of those rights need be included in the information provided to them, such as **the right to lodge a complaint with a supervisory authority**.

Regardless of the legal basis a victim support organisation uses, it must comply with the duty to **provide information about data processing** under the GDPR. This means that there is an obligation to inform the victim about:

- whether and how their personal data is processed;
- the legal basis for data processing, even if it is done in public interest,
- the period for which personal data will be stored,
- the right to request information about their data and its processing by the VSO,
- who it will be shared with[11]; and
- the right to demand rectification of incorrect data entries.

This information can be provided in a range of ways. Usually it will be most effective to provide this information using a combination of different methods: in conversation during the intake process, in written form through a leaflet that will be handed to the victim, as well as through providing a transparent privacy and data protection policy online.

Additionally, victims need to be informed about **subjects who will potentially receive their personal data**. Whenever possible, this information needs to be detailed – indicating precisely the entities which may be recipients. When that is not possible, the organisation may provide just categories of recipients. However, the victim support organisation/data controller must be able to explain why details cannot be given.

In the context of victim support, this may be justified by the fact that it is not possible to know, before an individual assessment, what type of further support a victim might need and who exactly will be able to provide such support. In such circumstances, the information on the categories of recipients should be as specific as possible by indicating the type of recipient (i.e. by reference to the activities it carries out, for example the data processors), the industry, and the location of the recipients.

[11] Complete list of information that must be provided to a data subject may be found in Article 13 GDPR

For example, if legal aid can be provided through a pro bono cooperation with a number of law firms, victims may be informed about the list of law firms with which the victim support organisation cooperates, with links to their respective data protection and privacy policies.

Victims also have the right to know whether and how their personal data is processed, to seek a copy of their data being kept by the support organisations and to **demand rectification** of incorrect data entries (Article 16).

Victims also have the right to demand erasure of their data which is stored and processed by the victim support organisation, the so-called **right to be forgotten** (Article 17). This right is not absolute and is applicable under a limited number of circumstances[12], such as:

- the personal data is no longer necessary for the purpose for which it was collected;
- data was collected based on consent which is now being withdrawn;
- data is processed based on legitimate interest which is disputed;
- data was processed unlawfully; or
- erasure is required by law.

Moreover, in addition to erasure, victims also have the right to demand **restriction of processing** of their data, in which case, the victim support organisation can retain and store the data. In this case, the organisation can only process such data with victim's explicit consent, the data subject's consent (if it is not the victim – e.g. the offender) or for the establishment, exercise or defence of legal claims or for the protection of the rights of another natural or legal person or for reasons of important public interest (Article 18). The restriction of processing is by definition only temporary. When there is a restriction to process data, case-management systems should provide for an option that restricted victim data is clearly marked as such and that any processing is disabled for the duration of the restriction.
Finally, victims also have the **right to data transferability** – which means that a victim can demand the support organisation to transfer their personal data to another service provider, where technically feasible (Article 20).

Data Retention

For victim support organisations, it may be especially difficult to determine for how long it may store the data of victims. While GDPR does not set a time-limit, personal data must be stored for the shortest time possible.

The retention period can depend on the circumstances of the case and the likelihood of extended need for support. Victims may return for additional support even years after the first contacts ended or may benefit from follow-up in situations likely to cause re-traumatisation.

[12] There are some other situations where erasure would be possible, however they do not appear to be relevant for victim support services and are hence not being mentioned here.

Of course, organisations can start a new case file, but this can be damaging for the victim as it will require them to recite their story again. Moreover, better connection and trust can be achieved, more quickly, where a support worker is already able to express knowledge and recollection of the case even where they didn't work on it. Effectively indicating to the victim that they haven't been forgotten.

For example, some associations of victims of terrorism contact victims of previous attacks to check up on them and the possible re-traumatisation they might experience in the case of a new terrorist attack even if it happens years after their own victimisation. To be able to do that, their data retention rules should enable them to keep victims' personal data on file.

This would suggest good justification for keeping data at least on some victims (those likely to have long term impacts) for a longer period of time – which would be established individually for each such victim.

That period should take into account the reasons why a victim support organisation needs to process the personal data, as well as any legal obligations to store the data for a fixed period of time (for example national labour, tax or anti-fraud laws requiring to store personal data for a defined period).

A victim support organisation may maintain contact with a victim for a period of time, and as long as the contact is maintained, a victim's personal data may be stored. The personal data may be further stored for an additional period of time for example to be able to complete and supplement statistics, to be able to receive feedback on quality of services. These are all legitimate purposes for data retention.

It should be emphasised that the main motive for victim support organisations to collect, store and share victims' data is to reduce secondary victimisation. If consent is seen as the principal, if not the only legal basis for storing and processing victims' data, and if it is strictly applied to every time the victim is contacting a support service – there is a great risk of secondary victimisation.

Once the retention period expires, the personal data should be deleted or anonymised for statistical purposes. This can be done through the process of pseudoanonymisation. This means that data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable person. For example, personal data (such as name, address, employment details etc) can be replaced by a random code or made-up names.

GDRP Compliant Referral to Specialised Services

There are three main channels for victims to initially access victim support services:

- On their **own initiative**, having had the knowledge of the service;

- At the **suggestion of the police** or other external actors (e.g. judiciary, health professionals etc.), who encourage victims to seek victim support services and possibly provide victims with information on where to find such services;
- Through **referral**, where authorities are empowered to collect victims' data and request victim support services to make the first approach to the victim.

Many victims will receive the support they need through a single contact with the victim support service. For many others, an individual needs assessment may indicate that the victim requires further support either internally in the victim support organisation, or through external referral to other organisations/institutions.

Referral should ideally be done directly between the referring and receiving organisation, in consultation with the victim. This means that once an individual assessment indicates that the victim needs further support, the victim support organisation will identify the appropriate provider of such service, forward necessary victim's data to the provider and inform the victim about the further steps.

In turn, the new provider will directly contact the victim, provide information about the organisation and offer their services. This referral process, carried out in collaboration with the victim, tends to have a higher victim take up rate compared with a victim being provided information about a service and being left to contact the organisation themselves.

It is important to keep in mind that in cases where support is provided through a network of victim support organisations which retain separate legal personality – as in that case victim is, for the purposes of GDPR, being referred to external service provider.

For example, where a victim needs legal representation, the support worker should be able to contact a law firm or a lawyer and share with them the necessary information about the victim, circumstances of the crime necessary for the provision of legal service and potentially indicate victims' vulnerabilities when they are calling to make an appointment for the victim. The lawyer can then contact the victim directly to request more details or documents and to make an appointment.

However, this is only possible where appropriate data protection and data sharing protocols are in place. Moreover, with respect to initial referral i.e. where a victim is referred to a victim support organisation for the first time, such as by the police, most successful referral systems are those termed **opt-out**, as opposed to opt-in.

With the opt-out system, a victim is informed that their information is automatically passed on to service providers unless they say they don't want it to be passed on. With the opt-in system, the victim is asked if they want their information to be passed on, and only where they agree does the referral happen.

Whilst the opt-out system seems to produce much higher take up of services, since GDPR, there has been increasing reluctance to rely on opt-out for fear of being non-compliant. This

comes largely from the faulty understanding that compliance is primarily ensured through consent and that it would be non-compliant to send victims' data under other legal bases.

Indeed, a victim should be informed about what type of data is being shared and with whom, under which conditions and for which purposes. However, this information can be presented in a number of ways and it does not mean that specific consent should be collected for every single possibility.

The list of third parties with whom the data may be shared should be included in a privacy notice and periodically updated. The crucial part is that a data subject is able to identify the controllers and the processors of their personal data. This information should be given to the victim the first time their personal data is collected. It can be done through providing a printed list, or sharing a link with the victim, briefly explaining to them why the list is being given and what the likelihood is of their data being shared.

Sharing the personal data with third parties on the basis of the legitimate interest criterion may be contested by the victim concerned. The legitimate interest basis is used where victims may reasonably expect that their personal data will be shared, for example with the provider of legal aid in civil proceedings, and where victims understand how their personal data will be used. Whether a victim truly understands the way his or her personal data is processed and expects to be passed onto a third party is subject to question and may be situation-specific.

It is important to note that a victim support organisation should have a written agreement in place with any third party with whom it shares personal data. It is also important to review the privacy policy of all third parties and that these policies contain:

- The subject matter of the processing;
- The duration of processing;
- The nature of processing;
- The purpose of processing.
- The type of personal data to be processed
- The categories of data subjects whose data is to be processed
- The rights and obligations of the data controller
- Certain instructions in case data is shared with a data processor:

Cross-Border referrals, including outside the EU

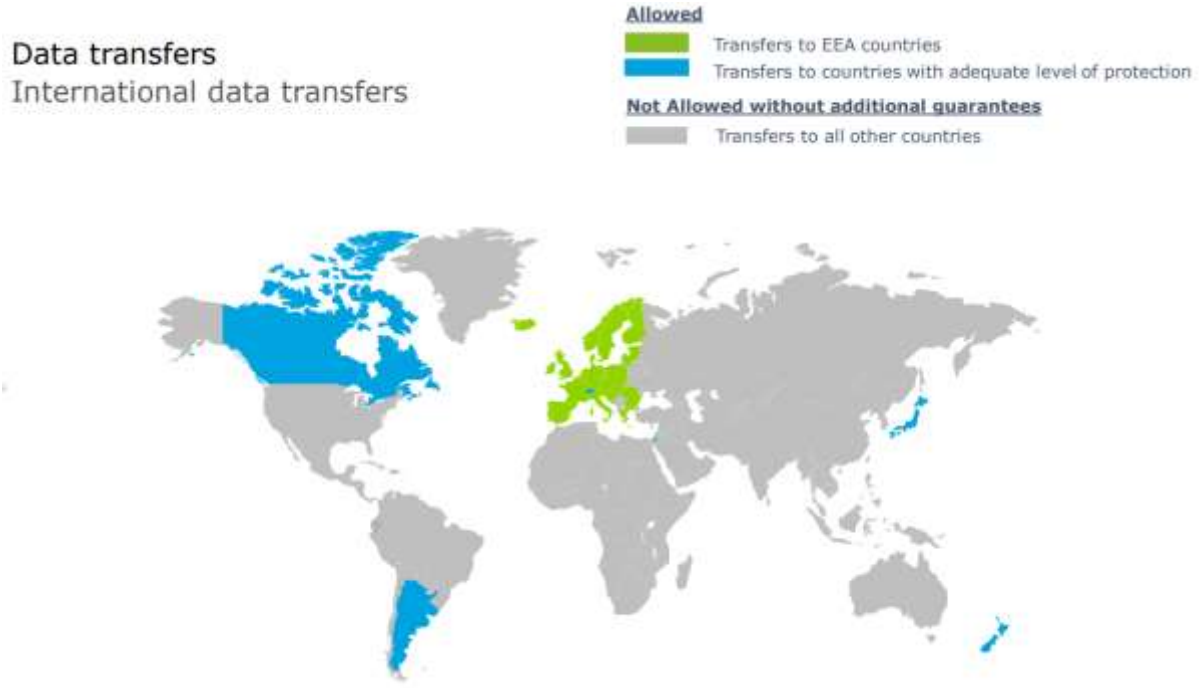
In case of cross-border referrals in the EU, the same principles apply as in the case of domestic referrals between service providers. However, in case a referral or the sharing of personal data takes place across borders outside the EU, the personal data may only be transferred to

a jurisdiction[13] or where a victim support organisation has implemented a lawful data transfer mechanism.

For example, the transfers are permitted if the controller or the processor adduces appropriate safeguards in the form of Model Clauses approved by the European Commission or national data protection authorities. Also, the transfer may take place on the basis of an approved Code of Conduct, together with binding and enforceable commitments to provide appropriate safeguards.

One may also base data transfer on certifications together with binding and enforceable commitments of a victim support organisation which shares the personal data to apply the certification to the transferred data. The personal data may be also transferred on the basis that the data subject, having been informed of the possible risks of such transfer, explicitly consents. Other legal bases may be applicable.

According to the latest information, only a small number of non-EU countries, as presented in the map below is considered to be GDPR compliant[14]:



In case of data transfer to other countries, to make sure that compliance is achieved, there should be a specific agreement with the entity in the non-compliant country, based on the

[13] Adequacy Decisions are subject to a periodic review, at least every four years, taking into account all relevant developments. The Commission can repeal, amend or suspend Adequacy Decisions for jurisdictions no longer ensuring an adequate level of data protection. See https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en.

[14] Image credit of: Deloitte Privacy Knowledge Center, Data Protection Officer Course, October 2020 Also, note that the UK might no longer be compliant after the expiry of the transitional period in January 2021.

model clauses, which are proposed by the European Union or on binding corporate rules (BCRs) – although the latter are only recommended for complex corporate structures. The list of model clauses is freely available and translated to all EU languages[15].

Special Categories of Data and criminal data

Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data or biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation is considered special categories of data, and processing such data is in general more limited.

In terms of processing special category data, victim services organisations should rely on domestic legislation and the individual circumstances of any case. In principle, special data should only be collected when it is necessary.

In this regard, it is possible to consider such processing that is necessary for reasons of substantial public interest, is proportionate to the aim pursued, respects the essence of the right to data protection and provides for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.

This may be justified when such type of data is fundamental for determination of the type of support to be provided to the victim – e.g. a transgender victim of hate crime who is being referred to a specific type of specialist services, or health data which is necessary for the provision of psychological support.

It may also be necessary to gather and process such data in order to capture the specific problems certain groups of victims face – e.g. hate crimes against certain ethnic groups, or specific support needs for victims with specific vulnerabilities. In each case, the victim needs to be informed about the fact that such data is being collected and maintain their data protection rights.

Victim information sheet

Based on the above, it is advised to provide victims with the specific information which will let them know how their data is being stored and processed and what their rights are regarding their personal data gathered by victim support organisations.

What information to provide to a victim of crime as regards the GDPR requirements?

[15] The full list can be found here: https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/standard-contractual-clauses-scc_en

- Contact details of victim support organisation;
- Purposes for which the personal data is collected (e.g. statistics, case-management, referral to other support organisations etc.);
- The type of personal data concerned (e.g. name, address, phone number, type of crime, circumstances of the crime, injuries suffered etc.);
- The legal basis for data processing;
- How long the data will be stored;
- Potential recipients of personal data;
- Whether the personal data will be transferred to a recipient outside the EU;
- Information about rights of data subjects/victim (such as the right to access personal data), the right to lodge a complaint with a data protection supervisory authority or the right to withdraw consent at any time;
- Where applicable, the existence of automated decision-making and the logic involved, including the consequences thereof.

Conclusions and recommendations

Privacy and confidentiality is a fundamental right that sits at the core of the work of victim support organisations. It is an intuitive cornerstone of a confidential and high quality service. It is why GDPR standards are a welcome reinforcement to this foundation.

Support to victims of crimes is an important societal service that engages and protects fundamental rights such as the right to life and justice. EU Member States have a legal obligation to make sure such services are available and fully accessible to all. Many countries now recognise that victim support is so important that it should remain open even as most others services are shutting down in the face of a lethal pandemic.

Achieving data protection and victim support is therefore a balancing act. It is critical that all **organisations working with victims understand their data protection duties and have in place the correct mechanisms**, procedures and training to respect obligations and protect victims.

Organisations must implement data protection rules without impeding support. In particular, this means **using the wide range of legal bases for the processing of data.**

Insisting on repeated collection of consent may be harmful for victims. Asking them to tell their story several times, repeatedly asking them the same questions, and giving them the same explanations over and over again, risks frustrating or potentially harming an already traumatised victim.

While **consent is a foundational element of working with victims**, relying solely on it to process their data can be bureaucratic, burdensome and can be counter productive. **Victim support services should therefore be fully aware of the opportunity to use all legal bases and should rely on those which fit best their situation and minimise burdens.**

Whilst these obligations rest on individual organisations, the reality is that the **EU data protection framework has not been designed with their situation in mind**. **Vague rules** and the broad **room for interpretation** left to national data protection authorities, has resulted in **legal uncertainty for victim support organisations.**

Overwhelmed with the pressures of limited funding and the increasing support needs of victims, organisations are left anxious about compliance. **The absence of legal certainty** and **fear of serious consequences can to lead to organisations providing fewer services** or **devoting limited resources to expensive solutions** that may not be necessary, just to be 'safe' from ruinous fines. This situation **risks the quality and effectiveness of victim support services**.

The EU, Member States and Data Protection authorities must join forces with support organisations to develop reasonable, balanced solutions that achieve the equally important objectives of data protection and support of victims.

Using EU co-operation mechanisms, dialogue between EU and national data protection authorities and victims support organisations should establish **clear, practical and feasible implementation guidance** so that operators are not working against a back drop of fear.

The EU and Member States should enable support organisations to rely on legal bases most suited to their situation. This should start with **the recognition of victim support providers as either the public interest services.** Indeed, any service which must be made available as a State obligation under EU law and which needs to remain available to all who need it, for as long as needed, is a public interest service.

Moreover, at least some of the victim support services are indeed provided in pursuit of compliance with a **legal obligation.** Some of them are already imbedded in the national legal systems by virtue of the Victims' Rights Directive, the Directive on the European Protection Order or the Countering Terrorism Directive, to name but a few possible sources of legal obligations.

Finally, it is should also be recognised that the **processing of victims' data is done in pursuit of a legitimate interest or even vital interest** where this ensures that victims receive the support they need and for as long as they need it.

Many victim support organisations operate in fear of potential fines for GDPR non-compliance at the expense of victims' wellbeing. A clear operating framework – based on legal certainty must be developed and **sanctions for non-compliance must take into account data protection and victim support objectives**, recognising the vulnerable financial situation of most organisations. **Sanctions should promote change and improvement, not result in the loss of critical services** or ineffective operation of those services.

Guidance on **data protection should enable easy, effective access to support**. In particular, this means ensuring that **GDPR does not stand in the way of safe referral mechanisms**. Ultimately, the combination of **appropriate data protection safeguards with the possibility of opt-out of referral should be consistently recognised across the EU as compliant with GDPR rules.**

Across the EU, victim support organisations are committed to protecting the data of victims whilst supporting them. They face multiple hurdles and uncertainties which are costly from a time, resource and financial perspective.

The EU, Member States and Data Protection authorities owe it to victims to simplify rules and help organisations to comply through a clear legal framework relying on the most appropriate legal bases, and with the provision of adequate funding for organisations' data protection mechanisms.