Guidance on Police Disclosure Following Road Traffic Collisions

Document information

Protective marking:	Official
Author:	Dean Hatton - Executive Business Manager
Force/Organisation:	NPCC Roads Policing
National Policing Coordination Committee Area:	Operations
APP/Reference Material:	Disclosure of Material to Third Parties | The Crown Prosecution Service (cps.gov.uk)
Contact details:	dean.hatton@sussex.police.uk
Review date:	31st July 2025
Version:	1.0

Any queries relating to this document should be directed to either the author detailed above or the NPCC Business Support Office on business.support@npcc.police.uk

Contents

Introduction and Background

1.1 Section 170 Road Traffic Act 1988[1] places a legal obligation on motorists involved in certain road traffic collisions to exchange their details namely, '*their name and address and also the name and address of the owner and the identification marks of the vehicle*' at the scene of the collision.

1.2 However, if for any reason this requirement to 'exchange details' does not occur at the scene of the collision then those involved must report the collision to the police to fulfil the requirements of s170 Road Traffic Act 1988 and to avoid committing a criminal offence.

1.3 This may occur when there is or has been some form of police investigation which can lead to criminal prosecutions or coronial processes, or equally when there is no requirement for a police investigation into a collision.

1.4 Very often therefore, police forces will hold information in relation to road traffic collisions that is relevant to civil proceedings, (insurance claims etc.). This may not only be names and addresses of drivers and vehicle details, but could also include witness details, CCTV footage and other investigation material that may contain personal data.

1.5 The Crown Prosecution Service (CPS) has published advice on Disclosure of Material to Third Parties | The Crown Prosecution Service (cps.gov.uk).[2] This advice sets out why early disclosure is important to assess the merits of the civil claim, issue court proceedings and seek interim payments of final damages, as soon as possible.

1.6 Notwithstanding the above CPS guidance, this NPCC 'Guidance on Police Disclosure Following Road Traffic Collisions' document is written to highlight the legal footing on which NPCC believes such disclosure can be made and supersedes all other documents that offer, or purport to offer advice on this specific matter from the 'police' perspective, including any document issued by the College of Policing.

1.7 This document does not interfere with the CPS guidance as described above, which forces should also refer to, nor the national charging policy for police reports in relation to road traffic collisions.

1.8 This document does not amount to legal advice.

[1] Road Traffic Act 1988 (legislation.gov.uk)
[2] Disclosure of Material to Third Parties | The Crown Prosecution Service (cps.gov.uk)

2. Data Protection – The Challenge

2.1 It is recognised that when the police collect a driver's name and address, the name and address of the owner of the vehicle involved in the collision, and the identification marks of that vehicle, voluntarily or otherwise, witness details and any other material that amounts to personal data, they are processing that personal data.

2.2 Consequently, any police processing or use of that personal data, including its disclosure, must comply with the Data Protection Act 2018 and UK GDPR requirements which apply to the use and processing of personal data.

2.3 The collection of this personal data may be regarded as processing for one or more of the 'law enforcement purposes' - defined at s31 of the Data Protection Act 2018 (DPA 2018) as *"…the purposes of 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"* – on the basis that collecting the information is necessary to avoid an offence under s170 Road Traffic Act 1988 being committed by the driver where they report the collision to the police, and more widely, while the police investigate the circumstances of a collision.

2.4 Any subsequent processing of personal data for law enforcement purposes must comply with the DPA 2018 rather than the UK General Data Protection Regulation (UK GDPR).

2.5 When personal data originally obtained for one of the law enforcement purposes is disclosed for civil litigation purposes that disclosure cannot be regarded as being for one of the law enforcement purposes. This is because the disclosure purpose would not fall under the s31 DPA definition and because the recipient will not be a 'competent authority' – only competent authorities can process for law enforcement purposes.

2.6 The Second Data Protection Principle in the DPA 2018 includes a requirement at s36(4) that "*personal data collected for any of the law enforcement purposes may not be processed for a purpose that is not a law enforcement purpose unless the processing is authorised by law".*

2.7 Consequently, a disclosure of personal data for the purposes of civil proceedings must be regarded as falling under the scope of the UK GDPR and therefore 'an authorisation in law' must be found to underpin the disclosure and satisfy s36(4) of the DPA.

3. An Authorisation in Law

3.1 There needs to be a lawful basis for any disclosure, this is fundamental. If there is no lawful basis, then the disclosure will be unlawful and could give rise to civil claims for breaches of data protection legislation.

3.2 The Road Traffic Act 1988 (RTA 1988) provides no lawful basis for the disclosure of personal data and cannot be relied on for this purpose.

3.3 The NPCC's position is that where disclosure following road traffic collisions is required for the purposes of civil litigation or prospective civil litigation an authorisation in law may exist due to the following:

- Common Law Policing Purposes – the nature of common law is that is not tightly defined
- Home Office Circular No. 81/1967 – paragraph 3 states: *"It is desirable that all forces should adopt the same practice in providing information about road accidents and similar accidents for the purposes of civil proceedings."*
- Human Rights Act 1998 (HRA 1998) – police forces as public authorities are prohibited from acting in a way which is incompatible with the Article 6 Right to a fair trial and the Article 8 Right to respect private and family life. Where the police alone hold information that is necessary for an individual to pursue a civil litigation claim, a failure to disclose it would breach the police's HRA 1998 obligations.
- Purpose of providing the information by the police – the RTA 1988 is silent on what the purpose of providing this information to the police is, (other than complying with s170 RTA 1988) or, what the police are expected to do with the information beyond recording it. It could be argued that there would be no point in the police holding the information unless they were to subsequently disclose it where necessary for the recipient party to pursue civil litigation.

3.4 If the above are considered not valid then a court order served on the police requiring disclosure would provide an authorisation in law.

4. Compliance with UK GDPR

4.1 Once an authorisation in law is available it is necessary to consider the obligations arising from the UK GDPR, most specifically the Data Protection Principles in Article 6, with regards to the disclosure which are:

a) *Consent*
The individual has consented to the sharing of the data for a specific purpose
b) *Contract*
The processing is necessary for contractual purposes
c) *Legal Obligation*
To comply with the law i.e. a court order
d) *Vital Interests*
The processing is necessary to protect someone's life
e) *Public task*
Process is necessary for you to perform a task in the public interest or for your official functions, and the task has a clear basis in law
f) *Legitimate Interest*
Processing is necessary for legitimate interests of a third party unless there is a good reason to protect the individual's personal data which overrides those legitimate interests. However, this cannot apply to public authorities proceeding data to perform their official tasks.

4.2 For disclosure following road traffic collisions, the relevant Article 6 condition is likely to be public task (e) as legitimate interests (f) cannot be used by public authorities.

4.3 The police will inform all witnesses that their statement may be used in any possible criminal or civil procedures, however it is important to obtain consent form the witness to disclose their statement.

4.4 Consent (a) may be withdrawn at any time thereby removing compliance with Article 6.

5. Requests for Disclosure

5.1 Requests for disclosure relating to road traffic collisions are generally made by the insurers of the vehicles involved in the collision, or the party's legal representatives and are requested for the purpose of reaching an early agreement as to who is at fault for the collision.

5.2 There are several reasons to try to establish fault at an early stage, not least the need to secure financial support for the deceased's family and / or the injured party (or indeed their families) or to arrange rehabilitation.

5.3 Even if a lawful basis for disclosure can be established, the disclosure of the material itself needs to be carefully considered. It should also be noted that although there may be a lawful basis to provide disclosure, that does not necessarily mean that it must be provided.

5.4 In addition, in some cases disclosure could give rise to harm to individuals whose personal data has been disclosed. In the most extreme cases perhaps, threats to life or assaults. This in turn could give rise to further civil claims.

5.5 When considering the basis for disclosure, the disclosure to the extent that it is made, is likely done so further to s.5 (3) of Schedule 2 of the Data Protection Act 2018.

The following provides exemptions from UK GDPR provisions:

(3) The listed GDPR provisions do not apply to personal data where disclosure of the data—
*(a) is **necessary** (emphasis added) for the purpose of, or in connection with, legal proceedings (including prospective legal proceedings),*
*(b) is **necessary** (emphasis added) for the purpose of obtaining legal advice, or*
*(c) is otherwise **necessary** (emphasis added) for the purposes of establishing, exercising or defending legal rights, to the extent that the application of those provisions would prevent the controller from making the disclosure.*

5.6 Ordinarily, when requesting disclosure, the purpose of the disclosure will be stated within the correspondence. If not, then it is permissible to respond by asking for the purpose of the disclosure.

5.7 It is important to note that if the disclosure is made, it is only for the purposes cited within s.5 (3) of Schedule 2 of the DPA 2018 and should not be used for any other reason.

5.8 Invariably, if the requests are made from insurance companies, law firms or other organisations as opposed to individuals, they should be aware of this. However, it would be good practice to remind the requestor when providing the disclosure, that it is only done so in accordance with s.5 (3) of Schedule 2 of the DPA 2018.

5.9 In situations where individuals make disclosure requests, disclosure may be made but the questions above still need to be considered and there is perhaps an increased risk when providing this information as it may not necessarily be used for the purposes of civil proceedings.

6. Disclosure Considerations

6.1 Pro-active, process driven disclosure relating to s170 Road Traffic Act 1988 and road traffic collisions is unlikely to be considered necessary as set out at paragraph 5.5 unless it is formally requested. This is because if no 'request' for disclosure has been made, it is difficult to establish and therefore argue why disclosure is *necessary*.

6.2 The information Commissioners Office (ICO) reminds the police of the questions that need to be considered when sharing personal data.

They are as follows:

1. Is sharing this information necessary?
   Are there alternatives to disclosure, which could also achieve the objectives?

2. Is the sharing of the information proportionate?
   Consideration needs to be given to any harm or detriment that may come from the sharing of this information. This needs to be considered in respect of what the objective of the disclosure.

3. What impact will this disclosure have on others?
   i.e. who else might be impacted by this disclosure. Risk assessments. Could there be an impact on others right of privacy?

4. The need to record the factors in the decision-making process. Including the lawful basis for disclosure.
   ICO expects that the police document the reasons for their decisions. This would include the lawful basis for the disclosure. This would need to be provided in the event an allegation is made of an unlawful disclosure

5. Seek the views of Data Protection officers.

6.3 Disclosure, relating to road traffic collisions, should only be made on request and should be made on a case by case basis.

6.4 All decisions to disclose should be subject to individual considerations and be documented in a retrievable format. This should include the authorisation in law and the GDPR Article 6 principle upon which the disclosure relies.

6.5 Where there is an ongoing criminal investigation disclosure requests must be referred to the Lead (or Senior) Investigating officer and the CPS for additional consideration as necessary.

6.6 Where considered necessary, additional safeguarding and risk assessments in relation to individuals whose details are to be disclosed should also be documented and be available in a retrievable format.

6.7 Forces should have due regard to the CPS Guidance Disclosure of Material to Third Parties | The Crown Prosecution Service (cps.gov.uk) which sets out provisions on where an Inquest or Criminal Prosecution is envisaged or pending or not, as the case may be, as well as time frames and other general provisions.

6.8 Other considerations:

- Forces should ensure disclosure is accurate and not excessive for the purpose of the civil proceedings
- Forces should ensure disclosure is done securely to a verifiable address (email or physical)
- Forces should respect any data subject rights applications made by the other party that may restrict disclosure
- Forces should ensure fair processing towards the person whose details are to be disclosed – consider specific privacy notice
- Forces should consider a record of non-disclosure is made
- Forces could consider the use of an application form
- Forces could consider only dealing with applications for disclosure from solicitors or insurance companies

6.9 If there any concerns on a particular case, further advice should be sought from force data protection and disclosure teams or force legal advice departments, and the CPS as necessary, before any disclosure is made.