DISCLOSURE TO NON STATUTORY INQUIRIES

ADVICE

The Church of England has initiated a non statutory inquiry into the circumstances where members of the clergy committed sexual offences against children.

I am asked to advise on the legal position of police forces receiving a request for information from that non statutory inquiry.

There is no statutory power held by a non-statutory body to compel the production of information to it. Therefore, any supply of information is made voluntarily by the police force concerned. In supplying that information the police force and individuals must act in accordance with the law to avoid the risk of committing a criminal offence and or creating a cause of action against a police force.

Forces might decide that they are not going to supply information in answer to such a request. A sensible reason for adopting such a position would be that the force is working with and supplying information to the statutory inquiry led by Justice Goddard and is using its resources to satisfy the demands of the statutory inquiry.

However, assuming that a force is not going to issue a blanket refusal then how is it to deal with a request?
DEALING WITH THE REQUEST

1. Ensure that there is clarity in the request and that it is fully understood.

2. Identify what material is held that might fall within the request.

3. Determine the source or sources of the material held.

Once those steps have been taken then the following must be addressed:

Does the disclosure of the requested information involve the risk of committing a criminal offence e.g. s19(4) of the Regulation of Investigatory Powers Act 2000? (unauthorised disclosure in connection with material to be kept secret) If it does then do not disclose it.

Does the disclosure of the requested information risk harming an important public interest e.g. the identity of a covert human intelligence source or prejudicing an investigation by the police or a prosecution. If it does then do not disclose it.

Does the disclosure of the requested information involve a breach of confidence? A party will be liable for breach of confidence if

(a) The material communicated to him had the necessary quality of confidence,

(b) It was communicated or became known to him in circumstances entailing an obligation of confidence,

(c) There was unauthorised use of that material

Coco v A N Clark (Engineers) Ltd (1969) RPC 41
Where a person gives the police an account of a sexual assault on them or another the police should assume that the material they speak about has the necessary quality of confidence to satisfy (a).

An obligation of confidence, “(b)”, arises and is confirmed in The Police (Conduct) Regulations SI 2012/2632 that provides in Schedule 2 Standards of Professional Behaviour under the heading “Confidentiality”

“Police officers treat information with respect and access or disclose it only in the proper course of police duties.”

To disclose without lawful authority would be an unauthorised use of that material and expose the force to a claim for breach of confidence (c).

Further, in personal matters, the protection of confidences and confidential information by the police, safeguards the right to respect for private and family life under ECHR Article 8 and a police force as a public authority must not act in a way incompatible with a Convention right.

In the light of the above, reference should be made to the SIO Guidance for Operation Hydrant which provides a route by which such information could be disclosed and that is with the consent of the person who has provided the information in so far as it relates to themselves and subject also to the Data Protection Act 1994. However, even then the public interest must be considered so as not to prejudice an investigation or prosecution by the disclosure.

DATA PROTECTION

The Data Protection Act 1994 “DPA” sets out a system to protect personal data. The obtaining and disclosure of personal data is “processing” personal data. The First Data
Protection Principle applies. In the absence of consent of the one or more data subjects in respect of personal data and or explicit consent of the one or more data subjects in respect of sensitive personal data there cannot be disclosure. In the absence of the necessary consent neither Sch. 2 para. 5 nor Sch. 3 para. 6 give relief from the First Data Protection Principle as it cannot be said to be “necessary” to disclose to the non statutory body. Unless the police can rely upon an exemption in S.29 the First Data Protection Principle cannot be escaped.

Under S.29(1) where the processing is for the purpose of prevention or detection of crime or the apprehension or prosecution of offenders the personal data is exempt from the First Data Protection Principle except to the extent to which compliance with Schedules 2 and 3 is required and to the extent where the application of Schedules 2 and 3 would prejudice the purpose. As I read it consent should be obtained but if that would prejudice the purpose then it does not have to be obtained. Nevertheless, that does not alter the purpose and I am not persuaded that supplying personal data to a non statutory inquiry is a purpose within section 29.

**PARTS OF THE DATA PROTECTION ACT 1998**

“Personal Data” means data which relate to a *living* individual who can be identified: (a) from those data; or (b) from those data and other information which is in the possession of, or is likely to come into the possession of, the data controller and includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual. S.1(1) Data Protection Act 1998.
“Sensitive Personal Data” means personal data consisting of information as to—

(f) his sexual life,

(g) the commission or alleged commission by him of any offence, or

(h) any proceedings for any offence committed or alleged to have been committed by him, the disposal of such proceedings or the sentence of any court in such proceedings.

S.4(4) Subject to section 27(1), it shall be the duty of a data controller to comply with the data protection principles in relation to all personal data with respect to which he is the data controller.

Principle 1
Personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless—

(a) at least one of the conditions in Schedule 2 is met, and

(b) in the case of sensitive personal data, at least one of the conditions in Schedule 3 is also met.

In respect of personal data (Sch. 2)

1. The data subject has given his consent to the processing.

5. The processing is necessary—

   (a) for the administration of justice,

In respect of sensitive personal data (Sch. 3)
1. The data subject has given his explicit consent to the processing of the personal data.

6. The processing—
   
   (a) is necessary for the purpose of, or in connection with, any legal proceedings (including prospective legal proceedings),
   
   (b) is necessary for the purpose of obtaining legal advice, or
   
   (c) is otherwise necessary for the purposes of establishing, exercising or defending legal rights.

S29.— Crime and taxation.

(1) Personal data processed for any of the following purposes—

(a) the prevention or detection of crime,

(b) the apprehension or prosecution of offenders, or

(c) the assessment or collection of any tax or duty or of any imposition of a similar nature,

are exempt from the first data protection principle (except to the extent to which it requires compliance with the conditions in Schedules 2 and 3) and section 7 in any case to the extent to which the application of those provisions to the data would be likely to prejudice any of the matters mentioned in this subsection.

(3) Personal data are exempt from the non-disclosure provisions in any case in which—

(a) the disclosure is for any of the purposes mentioned in subsection (1), and

(b) the application of those provisions in relation to the disclosure would be likely to prejudice any of the matters mentioned in that subsection.
“Data” means information which is recorded information held by a public authority [and does not fall within heads (1) to (4) above] S. 1(1) DPA 1998

A “public authority” means, amongst other things, a chief officer of police of a police force in England or Wales. (Freedom of Information Act 2000 s 3, Sch 1 para.59)

“processing”, in relation to information or data, means obtaining, recording or holding the information or data or carrying out any operation or set of operations on the information or data, including—

(a) organisation, adaptation or alteration of the information or data,
(b) retrieval, consultation or use of the information or data,
(c) disclosure of the information or data by transmission, dissemination or otherwise making available, S.1(1) DPA 1998

“Data Controller” means a person who (either alone or jointly or in common with other persons) determines the purposes for which and the manner in which any personal data are, or are to be, processed S.1(1) DPA 1998.

28 June 2016

Kevin Hegarty QC

St Philips Chambers

Birmingham | 55 Temple Row, Birmingham B2 5LS | t: +44 (0)121 246 7000
Leeds| 41 Park Square, Leeds, LS1 2NP| t: +44 (0)113 244 6691
London | 9 Gower Street, London, WC1E 6HB | t: +44 (0)207 467 9444