Second Study Commission

Civil Law and Procedure

63rd Annual Meeting of the IAJ – San José (Costa Rica)

Questionnaire 2020

HOW DATA PROTECTION RULES ARE IMPACTING ON CIVIL LITIGATION

In Nur-Sultan Kazakhstan we decided that in 2020, our Second Study Commission will focus on how data protection rules are impacting on civil litigation. We have limited the questionnaire to five questions and we expect to receive short but concise answers. The questions are as follows:

1. Do you store digital data in your jurisdiction?

The Scottish Courts and Tribunals Service ("SCTS") is the independent body corporate which provides administrative support to the Scottish Courts and devolved tribunals. In conducting its business the Scottish Courts, and hence, SCTS, become guardian to large amounts of data predominantly in relation to tribunal hearings and criminal and civil court proceedings. The vast majority of SCTS records are created from physical and metadata submitted to the organisation by members of the public, the legal profession and justice partners in relation to tribunal hearings and criminal and civil court proceedings. Accordingly some storage, use, and management of electronic data occurs.

There are a number of instances where the civil courts proactively use, store and seek electronic documentation and data.

For example some electronic case management systems for court records are used. The Integrated Case Management System ("ICMS"), is one example, and is a system which was adopted in the autumn of 2016 for all civil court business. It serves as an electronic repository of many civil case papers.

The use of digital technology is also an important feature of the arrangements for commercial actions raised in the Court of Session (Scotland's civil court which deals with claims over £100,000 or those of otherwise legal or significant importance). Unless the court orders otherwise, all documents required during the court action are submitted electronically by parties and uploaded to and stored on a secure electronic court process folder for use by the court. Similar procedures are being adopted for the lodging and use of

papers required for civil appeal hearings in the Inner House of the Court of Session (our civil appeal court).

Another example of the use of digital data is Civil Online, which is an online service available for use in our sheriff courts for our lowest level of civil claims (known as simple procedure cases, which cover monetary claims up to the value of £5,000). Civil Online allows users, who are registered with SCTS, to raise and/or respond to a claim and submit case documents online. It also enables the court to send documents to parties electronically instead of by post. Users can access up-to-date information about their case outside business hours and from a variety of electronic devices including mobile phones and tablets via the platform.

Court of Session Rolls (lists which detail forthcoming court business) are published daily from Monday to Friday. They contain limited information (case reference numbers, parties' names and agents' details) on live cases and are available on the website for a period of 12 weeks after the date of publication. Publication of the Rolls of Court is a requirement of the Rules of the Court of Session (Rule 6.1).

2. How is it stored and for how long?

Any digital information held by SCTS relating to a case is stored on secure SCTS IT systems, located within restricted access areas. In most instances electronic documents are stored in specific access-controlled Windows folders or case management systems. For commercial court actions, as noted above, a specific electronic process folder is created for each court action where documents are saved.

Arrangements for the handling, storage, destruction and preservation of electronic records within the civil and case management systems are defined within detailed records schedules, polices and Information Asset Registers within the SCTS estate (discussed further at answer to question 4).

When the electronic information is no longer required in accordance with legal requirements and internal guidelines and policy it will be disposed of appropriately and securely.
For example the electronic process folder of a commercial court action in the Court of Session, referenced at answer 1 above, will be retained for 6 months following final disposal of the action (including any appeal). It will be then be securely deleted.

Some aspects of every court case are, however, archived permanently by National Records of Scotland ("NRS") under SCTS's obligations under public records legislation (The Public Records (Scotland) Act 1937 and Public Records (Scotland) Act 2011). Generally all Court of

Session civil case records are sent for permanent archiving to NRS 5 years after the date of completion of the case. Records of Sheriff Court cases are transmitted in line with the relevant Court Records Schedule after 25 years. The time period are reviewed by the Keeper of the Records. SCTS and NRS are currently involved in discussions in regard to the content, format and transfer of any electronic records to NRS, given any transfer has historically been in respect of physical documentation.

3. Who has access to the digital data in your jurisdiction?

Judges and a restricted number of SCTS staff members are provided with access to the SCTS secure IT systems and folders mentioned above at answer 2, in order to allow them to carry out their functions. Who within SCTS gains access to those folders is reviewed and determined by relevant departmental managers. The various IT systems, email accounts and Blackberry/mobile devices are password controlled. PCs and laptops are logged out or "locked" when not in use and portable media is suitably encrypted. Internal emails containing information of a sensitive nature are identified as such with an appropriate protection marking in the subject field.

4. Are there digital data protection rules in place in your jurisdiction?

The General Data Protection Regulation ((EU) 2016/679) of the European Parliament and of the Council of 27 April 2016 ("GDPR") on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and the Data Protection Act 2018 set out the regime for data protection and data processing in the United Kingdom, including digital data. GDPR specifies particular principles which must be upheld.[1] As a public body, the SCTS is required by law to manage and adhere to the requirements of information law, and is a data controller for the purposes of the aforementioned regime, and is registered on the Data Protection Register held by the Information Commissioner for the UK.

[1] Including: I) Fair and lawful processing. The definition of the "processing" is very wide and includes the activities of those who read manual files, send emails, destroy unwanted data or store data. II) Requirements that a data controller must adequately communicate to the subject the fact that the data will be kept for processing, the purpose of that processing and the person to whom it will be disclosed. Purposes must be specified and lawful and data should not be further processed in any way which is not compatible with said purpose. III) Data must be adequate, relevant and not excessive. IV) Data must be kept accurate and up-to-date v. Data must not be kept longer than purposes require. vi. Data must be processed in accordance with data subject's rights. VII) Security measures must be implemented to ensure no unauthorised or unlawful processing of personal data against and against accidental loss or destruction of or damage to personal data. VIII) Transfer of data abroad must be safeguarded by a comparable data protection system in the receiving country.

The other main legislation and requirements that impact on SCTS, other than the Data Protection Act 2018 and GDPR include:

- The Official Secrets Act 1989
- The Freedom of Information (Scotland) Act 2002
- The Public Interest Disclosure Act 1998
- The Disposal of Court Records (Scotland) Regulations 1990
- The Civil Service Code
- The Public Records (Scotland) Act 1937
- The Public Records (Scotland) Act 2011.

At a more local level, the SCTS has its own robust Data Security Policy and Record Management Plan which covers the processing, handling, storing and destruction of data as required under the application legislation and policies. Members of SCTS staff are required to complete and pass mandatory e-learning course(s) regarding information management and security, on an annual basis.

The SCTS has adopted the UK Government security classification scheme for protective markings signifying the level of security that should be allocated to each document and is an accredited member of the Public Secure Network, which is a secure network used by other public bodies such as the prosecution service and Police Scotland to transfer sensitive data electronically. Where the retention and disposal of records is not otherwise governed by other retention schedules, legislative provision or the SCTS Records Management Procedure, centrally held records are managed in accordance with Scottish Government records management principles set out in its Record Management Manual.

5. Who covers the costs relating to the storage and protection of the digital data in your jurisdiction?

SCTS covers the costs relating to the storage and protection of digital information which it holds and is responsible for.