INTERNATIONAL ASSOCIATION OF JUDGES
2ND STUDY COMMISSION

Response from Canada

How data protection rules are impacting on the way judges work in civil litigation?

1. In your jurisdiction is a court considered to be a data controller for data protection law purposes in all, or any, of the following situations:

a. **When performing its judicial functions?** No.

b. **For purposes connected with the administration of justice, including the publication of a judgment or court decision, or a list or schedule of proceedings or of hearings in proceedings?** No.

c. **For purposes connected with the efficient management and operation of the courts and for statistical purposes?** In many cases, yes.

Data protection legislation across Canada is substantively similar in terms of application. These data protection laws apply to businesses and most government institutions, but do not apply to the judicial functions of our courts. Accordingly, when performing its judicial function, including release of decisions and details of hearings, a court is not considered a data controller for data protection law purposes.

The open court principle provides that, unless otherwise stated, all court proceedings and court records are publicly available. Courts have supervisory power over court records and determine the rules for public access. Guides concerning public access to court documents and proceedings are available on the court websites.

Judges also have discretion to make orders (such as a publication ban, sealing order, or an *in camera* hearing) to protect the privacy of individuals with respect to personal data. This discretion must be exercised in accordance with an established legal test, balancing freedom of expression with other important rights and interests (*Dagenais/Mentuck* test). These types of orders are exceptional in civil matters as the right to open courts generally outweighs the right to privacy. However, decisions released to the public are typically drafted in a way that eliminates or minimizes the inclusion of personal data. In certain civil cases, legislation requires a mandatory publication ban on any identifying information in a judgment, such as for some family law and child protection matters.

The laws around statistical data and the efficient management and operation of the courts vary between provincial and territorial jurisdictions. For most jurisdictions, court administration records are available under data protection legislation, and are subject to the data protection laws that ensure privacy of personal information. However, judicial administration records are excluded from the application of data protection laws.

2. In your jurisdiction does a data subject (e.g. a party to litigation, a witness, or a party whose interests may be

affected by the litigation) have a right to information regarding the processing of their personal data by or on behalf of the courts?

A data subject is notified through the court website regarding the usual processing of all personal data. The personal data, consistent with the open court principle, is generally accessible by the public, excepting in family matters and child protection matters.

In particular, parties to a proceeding and their counsel are permitted access to information (including personal data) included in the court file of their proceeding. A member of the public may also access the information included in the court file unless the law (statutory or common law) or a court order prohibits or restricts access. If a publication ban restricts access to information in a file, the person may access the information only after agreeing to comply with the ban and acknowledging that failure to do so is a criminal offence. Public access to information in a court file for family matters and child protection matters is more carefully controlled and restricted.

A data subject, in any civil matter, has the option to apply for a court order imposing restrictions on public access to their personal information. The open court principle, ensuring public scrutiny and transparency, often prevails and restrictions on public access are imposed only in exceptional cases.

3. In your jurisdiction does a data subject whose personal data is published in a court document such as a judgment,

have the right to seek rectification of allegedly inaccurate or inappropriately disclosed personal data?

This is highly dependent on the nature of the personal data that is allegedly inaccurate or inappropriately disclosed. If it is merely a clerical mistake or accidental slip that resulted in the inaccurate or inadvertent disclosure of personal data, then procedural rules allow judges to rectify the error. The person participating in the case, or the judge on their own motion, can submit an application to rectify the error. The judge has discretion over rectifying the error.

4. In your jurisdiction is personal data contained in a judgment or decision of a court, or in a list or schedule of proceedings or hearings, generally made accessible to the public? If so, are there exceptions and what are they? If not, is there a redaction requirement, or alternative requirement, to be implemented before a judgment / list /schedule can be published so as to safeguard the rights of data subjects?

The identity of participants in court proceedings is a matter of public record and, for the most part, individuals are not protected from being named in reasons for judgment. However, there are times when the privacy interests of participants in the judicial system outweigh the public interest of open justice, and decisions are anonymized.

Efforts are made by judges to reduce, or eliminate, personal information that is not pertinent to the decision. The Canadian Judicial Council has approved and published a protocol regarding eliminating this type of personal information from decisions. This

protocol recommends avoiding inclusion in a judgment of personal information, such as: year of birth, age, gender, sexual orientation, race, ethnic and national origin, country of birth and residence, professional status, occupation, marital and family status, religious beliefs and political affiliations. In exceptional cases, such as certain family and child protection matters, the judgments are anonymized before publication, and initials are used for parties' names. However, this does not always prevent the parties from being identifiable.

5.

(a.) How are complaints addressed in your jurisdiction concerning alleged breaches by the courts of the rights of data subjects?

As noted above, the data protection laws in Canada that protect the rights of data subjects do not apply to the judicial functions of our courts. However, courts have policies that protect case-related personal information, unlawful disclosure, and privacy breaches. If a data subject has a complaint concerning disclosure of their personal data, or other non-compliance with a policy, that complaint is generally referred to the court's senior administrative officer. There are policies in place to guide the officer in the event of an unlawful disclosure or privacy breach.

(b.) Does your jurisdiction have a person or body with special responsibility for the supervision of data processing operations of courts when acting in their judicial capacity?

There is no person or body with special responsibility for the supervision of data processing operations of courts when acting in their judicial capacity.

6. In your experience have data protection rules impacted adversely on your judicial independence? If so, how have they done so?

In my experience data protection rules have had no significant impact on my judicial independence. As noted above, data protection legislation does not apply to the judicial function of the courts. Rules and common law principles addressing requests for publication bans, sealing orders, and *in camera* hearings do apply to the judicial function of the courts, and guide judges in exercising discretion on these requests.