International Association of Judges

2nd Study Commission

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

Summary of Member Association Responses to 2023 Questionnaire

# Table of Contents

**The Questionnaire**

The 2023 questionnaire of the 2nd Study Commission invited Member Associations to respond to questions addressing the following theme:

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

*Question 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?

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?

c. For purposes connected with the efficient management and operation of the courts and for statistical purposes?

*Question 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?

*Question 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?

*Question 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?

*Question 5*

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

*Question 6*

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

## Member Association Responses

*Armenia*

**Question One:**

**a.** Armenian courts may carry out data checks when accepting a claim or an application, and; during the examination of the case either by mediation of the parties, or on its own initiative. **b.** An official electronic information system exists by which information pertaining to the work of the courts are published online, however it has been afflicted by an ongoing electronic problem since February 2023. **c.** Apart from the electronic system mentioned above, there are no other information means for judges, aside from a more general electronic system invested in the Republic of Armenia, which is available, albeit to a limited extent, to Armenian judges.

**Question Two:**

Parties to civil proceedings can freely obtain all the data contained in case materials or petition the court to request relevant information from the appropriate authorities. The same is true in respect of completed proceedings and archived cases.

**Question Three:**

This depends on the nature of the personal data being viewed inaccurately. A party must make an application to rectify. If the change would result in altering the essence of an already published judicial act, this would be prohibited.

**Question Four:**

The final judicial act usually reflects certain personal data of a person, including names, address, marital status, family composition etc. Judicial acts are published online, the only exceptions are those acts relating to *in camera* proceedings.

**Question Five:**

There is no body which generally exercises control over data proceeding functions by the courts. Complaints on human rights violations attributed are addressed to the Minister of Justice and the Ethics Commission of the General Assembly of Judges, and subsequently result in disciplinary proceedings at the Supreme Judicial Council.

**Question Six:**

Data protection rules have impacted adversely on Armenian judicial independence. Judges' actions both in- and outside of work are monitored, and data compiled is made publicly available. Such a practice endangers judicial independence.

## *Australia*

The response submitted on behalf of the Australian delegation relates exclusively to the Federal Court of Australia. It does not cover state level systems which are distinct.

**Question One:**

Obligations pursuant to Commonwealth data protection laws apply to the Federal Court only in relation to an act done/practice engaged in relation to the management and administration of the Federal Court's registry and office resources. Documents, records, and other material relating to court proceedings are exempt from those privacy laws, their use instead being governed through the Federal Court of Australia Act 1976, relevant rules of Court, and orders, directions, and determinations made.

**Question Two:**

Information about the personal information handling practices of the Federal Court in relation to the management and administration of the Federal Court's registry and office resources is published on the court's website. Individuals can obtain further information by contacting the Federal Court's privacy officer.

**Question Three:**

Unless the court has ordered the confidentiality of particular personal data, personal information may be published in a judgment and a data subject cannot of right seek rectification. However, a data subject does have the right to request amendment or annotation of the personal information that the court holds about the individual in the management and administration of the Federal Court's registry and office resources.

**Question Four:**

Personal data is contained in judgments or decisions of the Court and in lists/schedule of proceedings/hearings unless the personal data in question is subject to a confidentiality order.

**Question Five:**

The Court has a privacy officer to whom complaints can be made in respect of personal information that the Court holds about the individual in the management and administration of the Federal Court's registry and office resources.

**Question Six:**

Data processing rules have not impacted adversely on judicial independence.

*Austria*

**Question One:**

Various national procedural laws provide for data protection. Judicial activity constitutes a justification for data processing in civil proceedings. A series of relevant procedural laws govern data processing in the area of court proceedings, regulating data protection rights and obligations in that area. Data protection issues do not generally fall in the responsibility of civil courts.

**Question Two:**

Every person has, *inter alia* other rights, a right to rectification. In matters covered by the judicial activity of civil courts and judicial administrative cases settled in senates, an individual may only invoke these rights if and to the extent that the rights are reflection in the relevant legal instruments.

**Question Three:**

Where a person's fundamental right to data protection has been violated by a court in the exercise of its judicial activities, that person has the right to request a declaratory judgment on this violation within one year from the date the applicant becomes aware of the alleged violation.

**Question Four:**

Decisions of public importance by the Supreme Court are published online and in accordance with domestic law. Personal information is redacted. From 2022, the publication of second-instance decisions in civil and criminal cases has taken place. Such decisions are only accessible by judges and judicial staff. Search results are anonymised. Hearing schedules are not published.

**Question Five:**

Every person has the right to lodge a complaint with the Data Protection Authority following a breach in the processing of their personal data. The courts are not subject to its supervisory function. GDPR provisions also exclude this where processing is carried out by courts in the course of their judicial activities. Data protection violations can be asserted before ordinary courts within the framework of remedies available under the procedural law.

**Question Six:**

There has been no noticeable adverse impact upon judicial independence.

## *Azerbaijan*

**Question One:**

A court is considered to be a data controller for data protection law purposes connected with the administration of justice. Data protection law is applied in litigation, including the publication of verdicts and other judicial decisions.

**Question Two:**

Personal data of parties to legal proceedings is accessible only to the judge and the parties to those proceedings.

**Question Three:**

If an error occurs during the placement of data in the electronic system regarding any of the parties, it is possible to rectify the error upon their notification.

**Question Four:**

Court verdicts and decisions are accessible to those who have access to the system. Ordinary citizens not connected with proceedings do not have access.

**Question Five:**

Complaints regarding issues arising in electronic litigation may be addressed to the Department of Information Technologies at the Ministry of Justice.

**Question Six:**

If the data of the judge presiding over the process and the data of all participants becomes publicly accessible, it may pose a problem during decision-making.

*Benin*

**Question One:**

Beninese courts are responsible for the treatment of data and are not data controllers in the exercise of judicial functions. For purposes connected with the administration of justice, particularly the publication of judicial decisions or listings, Beninese courts are required to carry out analyses on the impact of envisaged data processing operations on the operation of personal data. Processing data for statistical purposes is prohibited unless it is carried out using anonymous data.

**Question Two:**

Courts must inform parties of the collection and processing of their data and the related purposes. However, in practice, this is not always the case, as litigants are often unaware of their rights in this area.

**Question Three:**

Data subjects have the right of rectification. To exercise this right, the interested party must send a dated and signed request to the relevant court which has 45 days to process it and communicate the rectifications or deletions made to the applicant.

**Question Four:**

Personal information generally appears in judicial decisions, court rolls, summonses and other relevant documentation. However, in sexual offending cases and criminal cases involving minors, personal data is omitted in published decisions.

**Question Five:**

In principle, persons affected by data protection violations have the right to file a claim or complaint with the Personal Data Protection Authority. To date, this body has not received any complaints from the courts, which is attributed to a lack of awareness on the part of litigants. There is no body supervising processing activities of the courts.

**Question Six:**

Data protection rules have in no way undermined Beninese judicial independence.

*Brazil*

**Question One:**

A court in Brazil is considered to be a data controller for data protection law purposes. Processing of personal data by courts is expressly covered by domestic data protection law. In all three situations envisaged by the question, the governing principle is set down by the Constitution of Brazil, namely that judicial activity is public with the only exception being cases conducted under a seal of confidentiality – which such cases are delimited by the Code of Civil Procedure (e.g., when demanded by public or social interest; concerning certain family matters; containing data protected by the constitutional right to privacy, and; concerning arbitration provided that the confidentiality agreed upon is proven before the court). Anyone can access the data of judicial proceedings except in such cases where only the parties and their lawyers have access to the process.

**Question Two:**

Data subjects (e.g., a party to litigation, a witness, or a party whose interests may be affected by litigation) have a right to information regarding the processing of their personal data by or on behalf of the courts.

**Question Three:**

According to the Brazilian Data Protection Law, a data subject whose personal data is published in a court document has the right to seek rectification of allegedly inaccurate or inappropriately disclosed personal data.

**Question Four:**

The rule is publicity of judicial acts. Data is available to the public in general except in cases that are processed under a seal of confidentiality, where only parties and their lawyers have access to the process.

**Question Five:**

Complaints about violations of data processing by the Brazilian courts can be addressed to a special commission designated by the courts for that purpose.

**Question Six:**

Data protection rules do not impact adversely on judicial independence.

*Bulgaria*

**Question One:**

The courts are considered data controllers in all situations identified in the question under the EU's GDPR. For efficient management of justice, courts are only considered data controllers in terms of processing labour law-related personal data, including when organising public competitions for recruitment of employees.

**Question Two:**

Data subjects have a right to information regarding the processing of their personal data as per the general EU law framework.

**Question Three:**

According to Bulgarian law, all publicised versions of the judicial acts have to be anonymised. Data subjects have the right to request anonymisation of public court records.

**Question Four:**

Published versions of all judiciary acts are always anonymised. The public has access to the names of the parties and other participants in the proceedings only as far as these are called in open court. Summons are handed to the parties personally with the exception of summoning through publication or affixing of a letter on the party's door, but in these situations generally the subject matter of the case cannot be inferred from the openly accessible text.

**Question Five:**

Every court has a data protection officer who handles such requests and general oversight is provided by the Inspectorate of the Judiciary. Complaints by data subjects can be filed to both. In circumstances of a breach, the aggravated party may file a civil compensation claim.

**Question Six:**

Not so far, although it can have adverse effects if scrutiny powers are abused. The system has some mechanisms to deal with that, including individual immunity of judges from civil or criminal actions against them by private parties, unless there has been intentional criminal activity, and the fact that the body controlling data protection issues is not part of the executive.

*Canada*

**Question One:**

In respect of parts a. and b. of question one, the Canadian delegation has answered "No". In respect of part c., Canadian courts are considered, in many cases, to be data controllers. Laws around statistical data and efficient management operation of the courts vary between provincial and territorial jurisdictions.

**Question Two:**

Parties to a proceeding and their counsel are permitted access to information included in the court file of their proceeding. A member of the public may also access the information included in this file unless the law or a court order prohibits or restricts such access.

**Question Three:**

If the breach concerned is merely a clerical mistake or accidental slip resulting in the inaccurate or inadvertent disclosure of personal data, then procedural rules permit judges to rectify the error. This can be done subsequent to the making of an application by the data subject, or by the judge of his/her own motion. The judge has discretion over rectifying the error.

**Question Four:**

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. Where privacy interests outweigh public interest of open justice, decisions may be anonymised. Efforts are made by judges to reduce/eliminate such personal information as is not pertinent to the decision. A Canadian Judicial Council protocol regarding such a practice is in circulation.

**Question Five:**

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, that complaint is generally referred to the court's senior administrative officer. There is no body with special responsibility for the supervision of data processing operations of courts acting in their judicial capacity.

**Question Six:**

Data protection rules have had no significant impact on judicial independence.

*Chile*

**Question One:**

The Chilean delegation answered in the affirmative in respect of each part of the question.

**Question Two:**

Data subjects have a right to information regarding the processing of their personal data by or on behalf of the courts.

**Question Three:**

Data subjects have a right to seek rectification of allegedly inaccurate or inappropriately disclosed personal data, which right may be exercised by way of judicial appeal for clarification, rectification, or amendment.

**Question Four:**

Personal data contained in judicial decisions and lists of proceedings are made accessible to interested parties by way of a digital platform. However, in family law cases or in criminal cases in which there is a special and exceptional witness protection at play, then this digital platform is not made available.

**Question Five:**

The Chilean Civil Service has responsibility for handling complaints regarding misuse of personal data.

**Question Six:**

Data protection rules have not adversely impacted on Chilean judicial independent. On the contrary, it is said that it benefits judicial work and allows the appropriate application of constitutional warranties to the process and to the individuals.

*Cyprus*

**Question One:**

Data processing rules do not apply in respect of courts performing their judicial functions. In respect of the administration of justice, the Supreme Court of Cyprus has issued two circulars providing guidelines to courts with regards to the publication of their decisions online. These include provisions relating to the disclosure of names of parties and witnesses and includes exceptions to the general rule of full disclosure e.g. in the context of proceedings concerning children and/or sexual offences victims etc. Courts are not considered data controllers in respect of the efficient management and operation or for statistical purposes.

**Question Two:**

According to a circular, a party, or a witness or any other person which, for good reason (e.g., medical condition, undercover police work, other sensitive personal data) wishes non-disclosure of any personal data that could reveal their identity has the right to apply to the court for remedy.

**Question Three:**

There is no express right contained in the circulars to seek rectification of allegedly inaccurate or inappropriately disclosed personal data. It is surmised that the courts have inherent power to examine and satisfy any such request – the courts generally have wide discretion over rectifying mistakes in a ruling or judgment, especially when it comes to clerical errors.

**Question Four:**

Court decisions are published in legal portals available to the public online. The only exceptions relate to the provisions of the aforementioned circulars e.g., references to parties' names.

**Question Five:**

A judge of the Supreme Court has been appointed to monitor the implementation of the circulars. Complaints can be directed to the Supreme Court in this regard.

**Question Six:**

Data protection does not affect judicial independence.

*Denmark*

**Question One:**

Danish courts are data controllers for the purposes set out in all three aspects of the question. Data protection laws comprise both EU (GDPR) and domestic legislation.

**Question Two:**

A data subject, any party whose interest may be affected by litigation, has a right to information regarding the processing of their personal data by or on behalf of the courts. This is regulated by supplementary rules in the Data Protection Act that applies alongside GDPR.

**Question Three:**

Data subjects have a right to seek rectification, both by procedural law and under the applicable data protection rules.

**Question Four:**

Judgments are publicly accessible subject to limitations regarding personal information contained therein. Redactions of sensitive personal information are made when public access is requested, save for where such information is a material detail having regard to the outcome of the verdict. The purpose of such redactions is to prevent the tracing of information back to the relevant person. Defendants' names are not published on lists on the courts' website of legal proceedings, and when court documents are published either online or otherwise made available to the public, parties' names are fully anonymised.

**Question Five:**

Data breaches are reported to the court's data controller after the head of department in the department that committed the breach has stopped the breach and informed parties to the case immediately by telephone and via e-mail. The data breach is assessed by the data controller, after which it is reported to the Court Administration which ensures that the court has handled the matter correctly.

**Question Six:**

There is no adverse impact beyond the certain additional workload associated with documentation to ensure compliance and which must be ready for presentation if there is an inspection by a data controller.

*Estonia*

**Question One:**

Answers given in respect of parts a. and b. of the question are in the affirmative. However, in respect of part c. regarding the efficient management and operation of the courts and for statistical purposes, the Estonian delegation has replied that the courts are not data controllers for such purposes.

**Question Two:**

Data subjects in Estonia, who are parties to litigation, witnesses, or parties whose interests may be affected by litigation, have a right to information regarding the processing of their personal data by or on behalf of the courts. §§ 22 to 24, inclusive, of the Estonian Data Protection Act is referenced in this regard.

**Question Three:**

Data subjects in Estonia do have the right to seek rectification of allegedly inaccurate or inappropriately disclosed personal data, other compensation if such breaches could not be prevented/cannot be eliminated as per § 7(1) of the Estonian State Liability Act.

**Question Four:**

As per §24 of the Estonian Constitution, court sessions shall be public, however a court may, pursuant to a procedure provided by law (The Code of Civil Procedure § 38) , declare that a session or a part thereof be close to protect a state secret or trade secret, morals or the private and family life of persons, or whether the interests of a minor, a victim or the administration of justice so require. Judgment is pronounced publicly except in cases where the interests of a minor, a spouse or a victim require otherwise. Anonymisation/Redaction of information may be sought on foot of an application or by the court's own motion.

**Question Five:**

The right of data subjects to request rectification and erasure of personal data is guaranteed under the Personal Data Protection Act. Estonia has a data protection and public information specialist both in first instance and appellate courts.

**Question Six:**

Data protection rules have not adversely impacted on judicial independence.

*France*

**Question One:**

The French delegation has answered in the negative in respect of each of the three parts of question one.

**Question Two:**

Data subjects do not have the right to receive information about the processing of their personal information by or on behalf of the courts. Generally, the National Commission on Informatics and Liberty (i.e. "CNIL") has jurisdiction to handle data processing-related claims.

**Question Three:**

A data subject can ask the court that rendered the decision to rectify a material error concerning his or her identity in a judgment, for example, but there is no real system for rectification of personal data of individuals, parties or witnesses. Generally, CNIL has jurisdiction. The French delegation note that EU Directive 2016/680 (i.e. "the Police-Justice Directive") places limitations on the rights of data subjects.

**Question Four:**

Judgments in France can contain very personal information. While a practice of anonymisation is pursued in the context of sensitive matters such as domestic violence cases, anonymisation is not a total guarantee against recognition by others.

**Question Five:**

Those with queries regarding data processing can contact the Data Protection Office at the French Ministry of Justice, which body remains the data controller for judicial databases. It is possible to contact the relevant court directly, but there is no suitable procedure for handling data processing complaints. CNIL has jurisdiction in the event of a refusal or failure to respond, however the scope of CNIL's jurisdiction does not extend to the jurisdictional act.

**Question Six:**

Concern is expressed that data protection rules can undermine judicial independence. It is said that online publication of judicial decisions "*calls into question the judge's office*", and the effect on the French judiciary of recent legislative developments in the area of data protection is noted.

*Georgia*

**Question One:**

Answered yes to all three parts of the question.

**Question Two:**

Data subjects who are parties to the proceedings, other interested third parties, witnesses etc. whose personal data is processed by the court or on its behalf have access to the information relation to this data processing, unless the information concerned contains a secret – including a state secret – data.

**Question Three:**

The data subject whose personal data was processed by mistake or incorrectly disclosed in a court decision has the right to request rectification in accordance with applicable procedural legislation.

**Question Four:**

During publication of court decisions, personal data is redacted. Only the names and surnames of disputing parties are indicated in schedules of court hearings. In the event that during the implementation of these procedures the personal data of any subject is processed by mistake, the data subject has the right to correct this error as well as to demand compensation for the damage caused.

**Question Five:**

The operation of the Georgian Law On Personal Data Protection does not apply to the processing of data for the purposes of legal proceedings in court, as this may harm legal proceedings before the final decision is made by the court. The entity defined by this law and equipped with special powers – the Personal Data Protection Service – does not supervise the process of personal data processing by the court in the process of justice implementation.

**Question Six:**

The obligation to protect personal data has no impact on judicial independence.

*Germany*

**Question One:**

German courts are considered to be data controllers for all three situations envisaged in the question.

**Question Two:**

All persons connected to court decisions have the right to information regarding the processing of their personal data.

**Question Three:**

Data subjects have the right to seek rectification of allegedly inaccurate or inappropriately disclosed personal data.

**Question Four:**

Personal data of parties is not normally publicly disclosed. Exceptions to this general rule include court notices e.g. schedules of proceedings, although there will be discretion for example in family proceedings or for endangered witnesses. This is the subject of judicial discretions. In certain legal areas, such as in bankruptcy, personal data will be published on a legal basis in a register free for all.

**Question Five:**

There is an internal check of breaches on privacy by the administration, and a Chief Information Officer ("CIO") to decide on complaints, which are quite rare. Most cases concern wrong handling in the post office e.g. regarding the sending of letters to other persons/institutions.

**Question Six:**

At this time, an adverse impact on judicial independence has not yet been observed. But there is a strong development to publish all court decisions and even to allow – in some cases – recording or even streaming of court proceedings. This might affect the judicial independence on behalf of public pressure.

*Greece*

**Question One:**

Greek courts are considered data controllers, with civil and administrative courts in particular falling under the scope of the GDPR. Criminal courts are considered data controllers under domestic law. Ultimately, where personal data is not anonymised, it falls under the scope of data protection laws.

**Question Two:**

Parties to civil proceedings may exercise all rights of information deriving from the provisions of Chapter III of the GDPR (in particular, Articles 12 to 15 inclusive). Third parties, or non-parties, or witnesses, who have legal interest in the outcome of the proceedings or where the processing of personal data does not affect them are not allowed to exercise these rights.

**Question Three:**

The rights to rectification, erasure and restriction of processing are provided to interested parties under Articles 16 to 18 of the GDPR.

**Question Four:**

As a rule, court decisions, acts, orders, etc. which are made publicly accessible are anonymised in a manner analogous with the approach of the Court of Justice of the European Union ("CJEU"). The same approach is adopted in relation to the drawing up of court tables and exhibits.

**Question Five:**

In line with the exception afforded to judicial and prosecutorial authorities in the context of their judicial function and duties, under Article 55 of the GDRP and equivalent provision under domestic law, the Greek Personal Data Protection Authority does not have competency in respect of controlling the processing of personal data by courts in the exercise of their judicial function. Data Subjects may, however, make a complaint regarding an alleged data breach occurring outside the scope of such exercise, to the aforenamed data protection authority.

**Question Six:**

No, both EU and domestic law exempt courts, when exercising their judicial function and duties, from oversight by data protection authorities.

## *Iceland*

**Question One:**

In respect of each aspect of this question, the Icelandic delegation has answered in the affirmative. They note, however, the role of the Judicial Administration institution which is responsible for the joint administration of the courts, and which, to the extent that that institution's work involves personal data, is deemed a data controller within the meaning of, and for the purpose of, domestic data protection legislation.

**Question Two:**

A data subject's right to information regarding the processing of their personal data is secured by general provisions of the GDPR.

**Question Three:**

The Judicial Administration has issued rules regarding the publication of judgments and rulings on court websites. Individuals can bring complaints regarding the publication of a court decision with their name or other identifiable information on the internet, such complaints shall be directed to the Chief Judge of the court that issued the decision. Data subjects have rights both to rectification and erasure.

**Question Four:**

Judgments are generally made accessible; publication of judgments being considered a core element of an open and transparent court system which is guaranteed by the Icelandic constitution and Article 6 of the ECHR. Balance is sought between this principle and individual privacy concerns relating to personal data. A policy of anonymising judgments and decisions prior to publication exists.

**Question Five:**

Icelandic courts are exempt under GDPR from the control of the national data protection authority when acting in their judicial capacity. This covers publication of judgments. There is no centralised body established to deal with alleged breaches by courts of the rights of data subjects.

**Question Six:**

Data protection rules have not had any special impact on judicial independence.

*Ireland*

**Question One:**

Irish courts are considered to be data controllers when performing judicial functions. However, for purposes outlined in parts b and c of the question, the Courts Service is the data controller.

**Question Two:**

Data subjects have a right to information regarding the processing of their personal data by or on behalf of the courts. However, this is subject to legitimate distinctions including the need to safeguard judicial independence/court proceedings.

**Question Three:**

A data subject has the right to seek rectification of allegedly inaccurate or inappropriately disclosed personal data, subject to legitimate distinctions including the need to safeguard judicial independence/court proceedings.

**Question Four:**

Judgments include parties' identities and necessary personal details and are made publicly accessible, as are all listings of proceedings. The Constitution requires justice to be administered in public, so all hearings are public save where an exception is provided for by law, e.g. cases involving minors. These proceedings are held in private, though bona fide representatives of the media are entitled to be present. Reporting restrictions apply to the identities of the parties, and they are anonymised in public listings and delivered judgments.

**Question Five:**

Complaints can be made to the Court Service in its capacity as data controller, and a dedicated judge has been assigned responsibility for ensuring that the data protection regime is implemented when courts process data in their judicial capacity.

**Question Six:**

Data protection rules have not had an adverse impact on judicial independence. However, it is observed that as Ireland operates a precedent-based legal system, the reporting of relevant facts is a central component of judgment-writing, and that the necessity to disclose as little personal detail as possible must be balanced by the necessity to disclose the basis of the reasoning in a case. Accordingly, extra care and thought must be taken.

*Israel*

**Question One:**

Israeli courts are considered to be “information managers”. This involves the maintenance of databases of different types of information relating to different legal procedures conducted and according to the type of use carried out. Judges and administrative staff receive training in preserving information.

**Question Two:**

A party to a proceeding is generally entitled to receive all the information that is before the court, except if there is evidence or certain information that was excluded by express authorisation in the law e.g. information regarding the mental state of a sex offence complainant, security offences, proceedings in family courts, etc. Third parties and media have the right to be present at court hearings which are generally held publicly, with exception to certain types of proceedings.

**Question Three:**

A non-party to a proceeding who believes that a judgment/decision concerning him has harmed him in any way or has published private issues affecting his good name may apply to the court with a request to limit publication, change the judgment, or censor the part concerning it.

**Question Four:**

A list of court hearings is generally open to the public; however it is not very accessible. This access issue does not affect the Supreme Court, the lists for which are accessible and published with regularity. Parties’ names are anonymised depending on the type of proceeding at issue, or parties’ names are accessible, but the hearing is *in camera*.

**Question Five:**

Depending on the type of breach, several actions might be taken: (i) submit an application to the judge hearing the case (regarding the manner of carrying out a judicial action), (ii) submit a complaint to the court’s secretariat (regarding the manner of carrying out an administrative action), (iii) submit a complaint to the Commissioner for Complaints about Judges (this action would relate to judicial conduct).

**Question Six:**

Rules of preserving information have not adversely affected judicial independence.

*Italy*

**Question One:**

Whereas the GDPR provides for an exception to courts acting as data controllers, when discharging their judicial function, domestic data protection law covers such functions. Accordingly, Italian judicial offices may be considering data controllers and processors in all of the situations indicated in the question. A distinction, however, is made between administrative and judicial data, the former type of data the subject of ownership by the Ministry of Justice, and the latter falling under the ownership of Judicial Offices.

**Question Two:**

Data subjects have the right to receive information about the processing of their personal data by or on behalf of judicial offices. These rights are governed by EU and Italian law.

**Question Three:**

Data subjects have a right to request rectification/erasure of personal data deemed inaccurate or improperly disclosed.

**Question Four:**

Judicial decisions are subject to redactions, following which they are made publicly accessible online. An interested party may request certain redactions prior to finalisation of a judgment. Alternatively, it may be judicially ordered that redaction/anonymisation of details takes place to protect the rights or dignity of persons concerned.

**Question Five:**

Complaints can be lodged through recourse to the judicial authority of to the Data Protection Supervisor. Appeal to the latter body cannot be made if the judicial authority is seized for the same object and between the same parties. Claims for compensation for pecuniary or non-pecuniary loss can only be brought to the judicial authority. No supervision of data processing operations by courts occurs when acting in their judicial capacity.

**Question Six:**

Data protection rules have not adversely affected Italian judicial independence.

*Japan*

**Question One:**

No courts are considered to be a data controller because Japanese data protection law is not applicable to courts. Courts have in place guidelines for handling personal information that they retain in association with the administration of justice. These have been established in the light of the purpose of the data protection law.

**Question Two:**

Data subjects do not have a right of information regarding the processing of their personal data by the courts because the data protection law does not apply to courts.

**Question Three:**

For the same reason as above, data subjects further do not have the right to seek rectification of allegedly inaccurate or inappropriately disclosed personal data.

**Question Four:**

Under the Code of Civil Procedure, any person may file a request to inspect a case record of civil litigation. Third parties may be restricted from accessing personal data if (i) it concerns a material piece of confidential information about the private life of a party, or (ii) it relates to a trade secret being kept by a party.

**Question Five:**

As aforementioned, data protection laws do not apply to Japanese courts. There is no body with special responsibility for the supervision of data processing operations of courts.

**Question Six:**

The Japanese data protection law has not affected judicial independence in Japan at all as courts are not captured by its scope.

*Kazakhstan*

**Question One:**

In the administration of justice collection, processing, protection of personal data of trial participants by the court is carried out in accordance with law. Judges and other court staff who become aware of restricted personal data shall ensure its confidentiality. The court is the controller of personal data protection in the administration of justice. The publication of the judgment or decision of the court, or the list or schedule of court proceedings or hearings in restricted proceedings shall be made by depersonalizing the personal data.

**Question Two:**

Every data subject (e.g. witness or litigant) has the right to information regarding the processing of personal data by or on behalf of the courts. This right is enshrined in Article 8-1 of the Law of the Republic of Kazakhstan on Personal Data and its protection. Through a public service, it is ensured that the subject is notified of actions with his/her personal data contained in judicial information objects.

**Question Three:**

The correction of inaccurate or misleading personal data in a court document is carried out by the court on the basis of an application by the subject or his/her legal representative. In civil cases correction of a typographical error is made in accordance with Article 235 of the Code of Civil Procedure by issuing a separate judicial act (ruling).

**Question Four:**

Personal data contained in a judgment or decision of a court, or in a list or schedule of proceedings or hearings, is generally public, except in cases classified as state secrets, personal, family, banking secrets, and other confidential information.

**Question Five:**

Complaints of alleged violations of data subject rights by the courts are considered in a general manner.

**Question Six:**

Judicial independence has not been adversely impacted by data protection rules.

*Latvia*

**Question One:**

In respect of each aspect of the question, the answer is that courts are not data controllers. However, the Latvian delegation notes that the Court Administration is the data controller for information necessary for judicial work. This limited access information stores in the Judicial Information System.

**Question Two:**

Data subjects can submit a data subject request to the Court Administration to find out information about the processing of personal data.

**Question Three:**

According to the Civil Procedure Law, a Latvian court may, upon its own initiative or upon an application of a participant in the case, correct clerical and mathematical calculation errors in the judgment.

**Question Four:**

Any person can use the publicly available part of the Judicial Information System to access lists of courts sessions, progress of their legal proceedings, anonymised court judgments or decisions, and progress data of other legal proceedings (however access to information regarding parties to such proceedings is precluded).

**Question Five:**

Data subjects have rights to submit a complaint to the Court Administration, as well as to submit a complaint to the national data supervisory authority. No person or body with special responsibility for the supervision of data processing operations of courts when acting in their judicial capacity exists. As the Judicial Information System comes under the remit of the Court Administration, this body is the addressee of complaints. That body's Operational Risk Manager and Data Protection Officer evaluates the complaint and provides recommendations to report a data protection violation to the Data State Inspectorate.

**Question Six:**

Judicial independence is not adversely affected.

*Liberia*

**Question One:**

The courts are not regarded as data controllers in all three situations envisaged in the question. This is on account of court documents being considered “public documents”.

**Question Two:**

All parties to litigation have the right to request from the Clerk of the Court, who is the custodian of the court’s records, to make copies of documents/information related to his/her case and provide same to him/her/them. This request may include information for personal data as well.

**Question Three:**

All parties to litigation have the right to seek rectification of information, especially personal data, which has been inaccurately or inappropriately disclosed. This request must be made through the office of the Clerk of Court for the attention of the judge with authority to order the rectification of the record/data.

**Question Four:**

There is no requirement for the publication of court judgments/decisions containing personal data. Once a judgment/decision of a court is made it becomes a public record. The Clerk of the Court stores and preserves the documents while submitting a copy thereof to the Record Section of the judiciary for documentation and statistical purposes.

**Question Five:**

Article 73 of the Liberian Constitution effectively precludes the establishment/appointment of a body/person with special responsibility to supervise data processing operations of courts when acting in their judicial capacity.

**Question Six:**

Data protection rules have not impacted on judicial independence in Liberia.

*Mexico*

**Translation Required.**

*Moldova*

**Question One:**

Moldovan courts are registered in the Register of Personal Data Processing, which is managed by the National Centre for the Protection of Personal Data. They are regarded as data controllers for all three purposes envisaged by the question.

**Question Two:**

A data subject has the right to information regarding their personal data, which they can exercise by filling a petition with the court involved in the litigation or with the Centre for Personal Data Protection.

**Question Three:**

Data subjects have the right to seek rectification, which can be exercised by submitting a written petition to the court where the document is filed. An employee from the court responsible for the integrated programme for managing cases will rectify the information immediately.

**Question Four:**

Courts may mandate redaction, either partial or complete, of specific personal information before publication. Judgments/decisions are posted on the judges' national portal where all information is accessible to the public with some exceptions, namely: date of birth, home addresses, personal identification numbers, and other information sufficient to identify the subject. Judgments/decisions relating to certain types of cases, e.g. family matters, sexual offending cases, espionage, invention patents, etc., are not posted.

**Question Five:**

Should the asserted violation pertain specifically to breaches of data protection regulations, the aggrieved party may reserve the right to lodge a formal complaint with the pertinent data protection oversight body. Upon receipt of such a complaint, this body undertakes a thorough review and, if justified, initiates corresponding corrective measures.

**Question Six:**

Data protection rules have never adversely impacted on Moldovan judicial independence. However, the potential for tension between safeguarding individual privacy and the need for transparency in the administration of justice is noted.

*Morocco*

**Question One:**

Moroccan law defines a data controller as an entity or individual who determines the purposes and means of processing personal data. To the extent that Moroccan courts fulfil such functions, they are data controllers for the purposes of parts a to b of this question.

**Question Two:**

The right to information regarding the processing of personal data is recognised as a fundamental principle of Moroccan data protection law.

**Question Three:**

Data subjects have the right to request rectification of personal data if it is inaccurate, incomplete, equivocal, or out of date. Such rectification, however, may be subject to limitations e.g. may apply only to factual inaccuracies and not to opinions/assessments contained in the judgment.

**Question Four:**

Judgments, court decisions, case lists or calendars are all made accessible to the public. The disclosure of certain personal data contained in these documents, however, may be subject to exceptions or restrictions laid down by law in order to protect the rights of data subjects. These restrictions may include anonymisation or redaction of sensitive information.

**Question Five:**

The National Commission for the Control and the Protection of Personal Data (i.e. “CNDP”) is responsible for supervising and enforcing data protection laws, including the processing of personal data by the courts. Affected data subjects may file a complaint with the CNDP which will investigate and take appropriate action, such as issuing recommendations, imposing sanctions, or taking legal action.

**Question Six:**

It is said that data protection rules may impact upon judicial independence if they are misapplied or over-interpreted. Questions may arise as to how courts handle and disclose personal data, and the need to protect individual privacy can conflict with transparency and access to justice. A balanced approach towards data protection and judicial independence is regarded as essential.

*The Netherlands*

**Question One:**

Dutch courts are data controllers for GDPR purposes in respect of data stored while performing their juridical functions enclosed to the cases, or the court decisions. However, they are not subject to a supervisory body in this regard. Dutch courts are also data controllers for purposes connected with the administration of justice. The Dutch delegation could not say whether the courts are data controllers for purposes described in part c. of the question.

**Question Two:**

Data subjects have the right to information regarding the processing of their personal data by or on behalf of the courts.

**Question Three:**

Data subjects do not have the right to seek rectification of allegedly inaccurate or inappropriately disclosed personal data, except in the context of a pending case.

**Question Four:**

A small portion of annual court decisions are published. This limited publication is attributed to a slow redaction process which is manually done. If decisions are published, they will be anonymised in line with guidelines. Only personal information pertaining to natural persons is redacted. Court hearings are normally accessible to the public, though family law proceedings, proceedings concerning minors, and proceedings disclosing very sensitive personal data may be exempt from this general rule. Lists of hearings are available for the press and anyone who requests them.

**Question Five:**

There is a body with special responsibility for the supervision of data processing operations of courts when acting in their judicial capacity.

**Question Six:**

Data protection rules have not adversely affected Dutch judicial independence.

*Norway*

**Question One:**

With respect to performing its judicial function, the courts are regarded as data controller only in respect of data stored while performing that function. They are not a data controller on a general basis. Norwegian courts are also regarded as data controllers in respect of purposes connected with the administration of justice, including publication of judgments or court decisions. The courts are not considered data controllers for the purposes connected with the efficient management and operation of the courts and for statistical purposes.

**Question Two:**

Data subjects have a right to information regarding the processing of their personal data by or on behalf of the courts.

**Question Three:**

There is no right to seek rectification of allegedly inaccurate or inappropriately disclosed personal data.

**Question Four:**

A judgment of decision of a court is made publicly accessible. Personal data disclosed in published judgments/decisions are normally anonymised, subject to judicial discretion.

**Question Five:**

There is a body with special responsibility for the supervision of data processing operations of courts when acting in their judicial capacity.

**Question Six:**

Data protection rules have not impacted adversely upon judicial independence.

## *Paraguay*

**Question One:**

Courts in Paraguay are regarded as data controllers for the purposes of parts a and b of the question. They are not regarded as data controllers for purposes connected with the efficient management and operation of the courts and for statistical purposes.

**Question Two:**

Data subjects have access to the system of jurisdictional management and to the case file in an electronic format. The right of data subjects to access personal information is provided for under Paraguayan law, and administrative and judicial bodies are under an obligation to ensure easy access and possibility of access.

**Question Three:**

Data subjects have the right to seek rectification, it is incidental to their right to appeal to obtain any modification of material errors or inaccuracies in the judicial resolution.

**Question Four:**

Paraguayan data protection law qualifies personal information by its availability by public information sources with no distinction nor classification of management types related to the personal information's content. Where conflict arises, a balance must be struck with other systems' principles, because the general reference to "*public information*" does not clarify what data falls under this umbrella term. Examination of personal data must be done based on other rules that define personal data and sensible personal data, that prohibit the publication of sensible personal data, and that establish "*the duty of secret*".

**Question Five:**

A court only receives data protection complaints in the framework of judicial processes. There is no independent oversight body, however the judiciary counts with "*denouncement channels*", that receive complaints relating to judicial management.

**Question Six:**

No adverse effect on judicial independence is reported.

*Philippines*

**Question One:**

Philippine courts are regarded as data controllers in all three situations envisaged.

**Question Two:**

Data subjects, including parties, witnesses, and legal representatives, have a right to information regarding the processing of their personal information. Data subjects provide information on a voluntary and wilful basis, and this information forms part of the case records. Data subjects are made aware that this information will be used for the service of notices, orders, resolutions, and the decision.

**Question Three:**

Data subjects have the right to rectification and erasure under Philippine law.

**Question Four:**

Publication/disclosure of personal data contained in court records is generally avoided. Confidential information as defined by Philippine law cannot be made available to the public. Redacted versions of decisions, resolutions or orders are prepared in the context of rape, child abuse, human trafficking, and other sensitive crimes. The name of the victim(s) in such cases are usually substituted with a fictional initial and the personal circumstances are removed.

**Question Five:**

The right to file a complaint is encompassed in domestic provisions regarding the right to information. A data subject may seek relief through submitting a formal complaint with the Municipal Court Information Officers ("MCIOs"), also referred to as Clerks of Court ("COCs") for cases concerning lower courts. Data subjects may also lodge a complaint before the National Privacy Commission in respect of alleged violations contrary to the Data Privacy Act 2012.

**Question Six:**

No, data protection does not affect judicial independence adversely.

## *Portugal*

**Question One:**

Portuguese courts are not data controllers when acting in the course of their judicial functions. Management of data is conducted by a court on a case-by-case basis, and when it comes to the publication of judgments, care is taken to anonymise/redact personal information.

**Question Two:**

Proceedings are public and the parties (and their lawyers) have access to the information contained in the relevant court file. Publicity of proceedings entails the right to examine and consult the case file electronically, to obtain copies or certificates of any documents incorporated therein. Under domestic law, access of information may be restricted with respect to personal data that is not relevant to the resolution of the dispute. Restriction is the subject of judicial discretion.

**Question Three:**

Clerical errors resulting in inaccurate or inadvertent disclosure of personal data may be rectified on foot of an application made by the concerned person to the relevant judge.

**Question Four:**

As a rule, proceedings and hearings are public. However, in the higher courts, published decisions are anonymised.

**Question Five:**

No specific body has been established to supervise the activities of the courts acting in the exercise of the judicial function. The higher courts, as well as the Councils, have appointed Data Protection Officers with duties limited to the processing of data carried out in the exercise of their administrative, management or internal organisation activities. Lower courts endeavour to put GDPR into practice, in collaboration with the Data Protection Officer appointed by the Superior Council of the Judiciary.

**Question Six:**

Data protection rules have no impact on judicial independence.

*Romania*

**Question One:**

Each court is registered in the Register of Personal Data Processing, managed by the National Supervisory Authority for the Processing of Personal Data. The courts process personal data for the purposes of exercising judicial and administrative functions.

**Question Two:**

The data subject has the right to obtain from the court a confirmation/denial of the processing of personal data and, in the case of an affirmative answer, has the right to access such data and information on how it was processed. With regard to the information on the names of the parties in a court file, it can be obtained by consulting a court portal, except where such information has been anonymised.

**Question Three:**

Data subjects have the right to obtain, without undue delay, the rectification of inaccurate personal data concerning him/her. A written request to the court where the file is located must be submitted, and if it is found that the personal data in question has been published inaccurately or incompletely, the request is admissible.

**Question Four:**

Personal data contained in judgments is redacted/anonymised including parties' names. Personal data contained in the hearing lists, are published only to the extent that parties do not request that files be "*confidential*" or that personal data be protected.

**Question Five:**

The Superior Council of Magistracy is vested with supervisory and control powers in respect of the personal data processing activity by Romanian courts in the exercise of their judicial powers. This includes duties of monitoring and verifying the personal data processing activity of courts. Data subjects may submit a complaint to this body where they do not receive a response to a request/complaint regarding the processing of personal data directed to the court where the file is located, within the legal term to make such a request. The Council has a wide array of remedies at its disposal.

**Question Six:**

Romanian judges do not report an adverse impact on their judicial independence.

*Serbia*

**Question One:**

In respect of part a. courts are only data controllers when performing judicial functions in the context of administrative disputes. As for part b., courts are data controllers and must announce allocation of cases, schedules of hearings within procedures that took place before every court, as well as anonymised decisions that have been adopted. And, part c., data is used by courts both for efficient management and for statistical purposes. Access to data is enable in accordance with domestic legislation.

**Question Two:**

The Serbian Constitution (Article 42 thereof) stipulates that the processing of personal data is solely regulated by laws, which also prescribe its goal and purpose, as well as the operator's obligation to inform every data subject of the processing of their data.

**Question Three:**

Data subjects have the right to seek rectification of allegedly inaccurate or inappropriately disclosed personal data.

**Question Four:**

Every judicial decision is anonymised in a way that personal data is not disclosed to the public. This is regulated by the Courts Rules of Procedure, adopted by the Minister of Justice.

**Question Five:**

Every breach of rules on personal data protection can be subject to inspection by the Commissioner for (Information of Public Importance) and Personal Data Protection. Should a person who has requested for inspection to be conducted be displeased by the Commissioner's decision, they have the right to court protection in an administrative dispute. This does not exclude the possibility for the person concerned to request compensation from the operator.

**Question Six:**

Data protection rules have not adversely affected judicial independence.

*Slovenia*

**Question One:**

Courts process personal data both when performing their judicial functions, as well as within the scope of judicial administration. In these respects, it is said that Slovenian courts are data controllers. In respect of part c. it is said that "*this is not foreseen in Slovenian law*".

**Question Two:**

Where data is processing for purposes connected with the judicial function, a data subject may exercise rights guaranteed by the GDPR only to the extent and in the manner specified by the laws governing the legal proceedings in his case. As regards where courts process data in the performance of administrative tasks, a more expansive range of rights is described including rights to information and erasure.

**Question Three:**

A data subject may request rectification by using objections, ordinary or extraordinary legal remedies, in accordance with the laws governing the judicial procedure in his case.

**Question Four:**

Court proceedings are, for the most part, public. Parties to proceedings must expect that certain personal details may be disclosed in the course of those proceedings and may be the subject of journalistic reporting. Within the courts, only persons who are entrusted to the management of proceedings have access to personal data. Personal data of parties or other participants may be forwarded to *inter alia*, other parties in the proceedings, other courts, the media/general public, to state and public bodies upon proven legal grounds.

**Question Five:**

In respect of data processing operations connected with the performance of judicial functions, no supervisory body exists. However, the same is not true in respect of such operations connected with administrative tasks, in which case complaints can be made to the Information Commissioner of the Republic of Slovenia against the data controller's behaviour.

**Question Six:**

Data protection rules have not adversely affected judicial independence in Slovenia.

*Spain*

**Question One:**

The Spanish delegation answered in the affirmative.

**Question Two:**

Data subjects have a right to information regarding the processing of their personal data by or on behalf of the courts.

**Question Three:**

Data subjects have the right to seek rectification of allegedly inaccurate or inappropriately disclosed personal data.

**Question Four:**

When publication of judicial resolutions is made, the resolutions with sensitive content are appropriately anonymised in a way that the parties are unidentifiable.

**Question Five:**

In Spain the Data Protection Supervision and Control Board of the General Conseil of the Judicial Power fulfils the oversight role described in the question.

**Question Six:**

It is said that, in principle, the treatment of data can make the management of cases more difficult and can also limit information, even though this limitation is not produced in the scope of the exercise of jurisdictional activity, but against third parties, so it does not limit Spanish judicial independence.

## *Taiwan*

**Question One:**

Taiwanese courts are data controllers for the purposes outlined in the question.

**Question Two:**

Those who are legally requested to read the court file may request copy of same, for a fee. A party may apply to the court clerk for inspection of, copying of, or photographing of the documents with expenses advanced. Third parties may apply, only with parties' consent. Where the material in question pertains to a private or business secret of a party or third party likely to result in substantial harm if disclosed, the court may on its own initiative deny the application or restrict its scope.

**Question Three:**

Under the Taiwanese Code of Civil Procedure, only obvious mistakes may be corrected. As such, a right to rectification exists in principle but it is subject to judicial discretion. In any event, in order to protect sensitive personal information, a judge may redact inappropriately disclosed personal data in a judgment.

**Question Four:**

Personal data contained in judgments is redacted prior to publication, particularly if its inclusion may easily identify the individual concerned. The exception to this is the inclusion of the natural person's name. However, even this may be redacted in some cases, most notably involving sexual assault or juveniles. Further redaction may be the subject of judicial discretion.

**Question Five:**

There is an Information Centre with special responsibility for the supervision of personal data in each court. Data subjects whose personal information was inaccurately published or used without due authorisation may seek rectification through the submission of a formal complaint with this body or to judges directly.

**Question Six:**

Data protection rules have not adversely impacted upon Taiwanese judicial independence.

*United States of America*

**Question One:**

In respect of parts a and b, concerning the exercise of judicial functions and purposes connected with the administration of justice, it is said that generally clerks of court fulfil the role of data controllers. As for part c, the American delegation responded by saying that a court is not regarded as a data controller for purposes connected with the efficient management and operation of the courts and for statistical purposes.

**Question Two:**

Data can be accessed by the public through the Federal Judiciary's electronic records database and filing system (i.e. "PACER"), unless otherwise restricted by court order. Users of this system are made aware of the system's privacy policy which describes how information is collected and stored. Data subjects can request that a court restrict access to their personal data by way of motion filed with the court.

**Question Three:**

Data subjects can file a motion for modification, removal of a court opinion or other document from public access, or rectify inaccuracies in the record.

**Question Four:**

Court dockets, documents, and opinions are generally presumed to be public, however they may be redacted to remove personal identifiers prior to publication on PACER. Federal rules and legislation govern requirements for confidentiality and specify procedures for attorneys and court reporters/transcribers to accomplish the required redactions.

**Question Five:**

Complaints may be submitted to the clerk of court of the particular court within which the alleged breach arose or the Administrative Office of the U.S. Courts for review and consideration.

**Question Six:**

Data protection rules have not been observed to have impacted adversely American judicial independence at the Federal level.