Antitrust Division

Privacy Impact Assessment
for the
Antitrust Division
Relativity One
(ATR SaaS RelOne)

Issued by:
Sarah Oldfield
ATR Senior Component Official for Privacy

Approved by: Andrew J. McFarland, Senior Counsel
Office of Privacy and Civil Liberties
U.S. Department of Justice

Date approved: August 17, 2026

(March 2025 DOJ PIA Template)

Section 1: Executive Summary

ATR SaaS RelativityOne (ATR RelOne) is a FedRAMP-authorized, cloud-based case management database system used to process, analyze, manage, maintain, and produce large volumes of data in connection with the Antitrust Division's litigation and investigation functions. The system is supported by ATR's Litigation Support Section and is accessible to authorized internal DOJ federal and contractor personnel, as well as a strictly controlled set of external users.

ATR conducts civil investigations, affirmative civil litigation, grand jury investigations, criminal prosecutions, employment matters, and FOIA processing. ATR collects documents, data, and testimony from subjects, targets, opposing parties, and third parties through civil investigative demands, search warrants, civil and grand jury subpoenas, and discovery requests, and ingests that material into ATR RelOne for case assessment, fact management, search, review, production, analytics, and legal holds.

ATR RelOne is owned and maintained by Relativity under license to DOJ ATR. As the FedRAMP-authorized cloud service provider, Relativity manages the platform infrastructure, hosting environment, and all security controls implemented within the CSP boundary; ATR is responsible for user management, access provisioning, permission administration, and all controls within the customer operational boundary. The platform is hosted exclusively within Microsoft Azure Government (US Gov Virginia region); data is never stored outside the United States. The system employs a hierarchical, multi-layered authorization model and a customer lockbox feature that restricts Relativity personnel from accessing ATR instances absent explicit ATR clearance and permission.

ATR RelOne includes both traditional artificial intelligence features (Technology Assisted Review, communication analysis, and automated redaction) and generative artificial intelligence through Relativity aiR, a suite of products built on Microsoft Azure OpenAI services that supports document review, privilege review, and case strategy. All AI-generated analyses and recommendations remain subject to qualified legal professional review and are designed to augment, not replace, human decision-making.

Section 2: Purpose and Use of the Information Technology

2.1 Explain in more detail than above the purpose of the project or information technology, the type of technology used (e.g., databases, video conferencing, artificial intelligence, machine learning, privacy enhancing technologies), why the information is being collected, maintained, or disseminated, and how the information will help achieve the Component's purpose, for example, for criminal or civil law enforcement purposes, intelligence activities, and administrative matters, to conduct analyses to identify previously unknown areas of concern or patterns.

ATR RelOne is ATR's cloud-based electronic discovery and case management platform. Its purpose is to ingest, organize, review, analyze, and produce the documents and data ATR collects in its investigations and litigation so that ATR can enforce the antitrust laws. Information is collected, maintained, and disseminated to support case assessment,

document and privilege review, fact and legal-hold management, analytics, and production to courts and opposing parties.

The types of technology used include a cloud Software-as-a-Service (SaaS) case management database built on the Microsoft .NET Framework and Microsoft Structured Query Language (SQL) Server, containerized microservices on Azure Kubernetes Service, and analytics capabilities. The system also employs artificial intelligence. Traditional AI features include Technology Assisted Review, communication analysis, and automated redaction of imaged content and electronic documents in their original format (e.g., Microsoft Word documents). Generative AI is provided through Relativity aiR, built on Microsoft Azure OpenAI services, which supports document review, privilege review, and case strategy. These AI features are used to replace error-prone manual processes and to improve efficiency and accuracy in document review, privilege review, and case-preparation activities, with qualified legal professional review of all AI outputs.

The information collected may contain a wide range of PII about members of the public and, in employment and procurement matters, about DOJ and other federal personnel. Because ATR's investigative and litigation collections are broad, almost any category of PII may be implicated in a given matter.

2.2 Indicate the legal authorities, policies, or agreements that authorize collection of the information. (Check all that apply and include citations/references.)

Authority	Citation/Reference
Statute	Antitrust Civil Process Act, 15 U.S.C. §§ 1311-14; Hart-Scott-Rodino Antitrust Improvements Act, 15 U.S.C. § 18a (§ 7A of the Clayton Act)
Executive Order	
Federal regulation	The Antitrust Division (ATR) has authority for the project under 28 C.F.R. §§ 0.40 (General functions) and 0.41 (Special functions).
Agreement, memorandum of understanding, or other documented arrangement	License agreement between DOJ ATR and Relativity ODA LLC for the RelativityOne SaaS platform.
Other (summarize and provide copy of relevant portion)	Federal Rules of Civil Procedure and Federal Rules of Criminal Procedure regarding discovery, disclosures, and subpoenas

Section 3: Information in the Information Technology

3.1 Indicate below what types of information that may be personally identifiable in Column (1) will foreseeably be collected, handled, disseminated, stored and/or accessed by this information technology, regardless of the source of the information, whether the types of information are specifically requested to be collected, and whether particular fields are provided to organize or facilitate the information collection. Please check all that apply in Column (2) and indicate to whom the information relates in Column (3). Note: This list is provided for convenience; it is not exhaustive. Please add to "other" any other types of information.

(1) General Categories of Information that May Be Personally Identifiable	(2) Information is collected, processed, disseminated, stored and/or accessed by this information technology (please check each applicable row)	(3) The information relates to: A. DOJ/Component Employees, Contractors, and Detailees; B. Other Federal Government Personnel; C. Members of the Public - US Citizens or Lawful Permanent Residents (USPERs); D. Members of the Public - Non-USPERs	(4) Comments
Example: Personal email address	*X*	*B, C and D*	*Email addresses of members of the public (US and non-USPERs)*
Name	X	A ,B, C and D	Names may be collected in association with a specific litigation or investigation.
Date of birth or age	X	A ,B, C and D	
Place of birth	X	A ,B, C and D	
Sex	X	A ,B, C and D	
Race, ethnicity, or citizenship	X	A ,B, C and D	
Religion			
Social Security Number (full, last 4 digits or otherwise truncated)	X	A, B, C and D	SSNs are collected for DOJ personnel. SSNs may also be included in case information from outside entities, although SSNs are not actively collected or requested.
Tax Identification Number (TIN)	X	A, B, C and D	
Driver's license	X	A, B, C and D	
Alien registration number	X	A, B, C and D	
Passport number	X	A, B, C and D	
Mother's maiden name			
Vehicle identifiers	X	A ,B, C and D	License plate numbers may be detected in video footage provided during investigations or surveillance.
Personal mailing address	X	A, B, C and D	
Personal e-mail address	X	A, B, C and D	
Personal phone number	X	A, B, C and D	
Medical records number	X	A, B, C and D	
Medical notes or other medical or health information	X	A, B, C and D	
Financial account information	X	A, B, C and D	
Applicant information	X	A, B, C and D	
Education records			

(1) General Categories of Information that May Be Personally Identifiable	(2) Information is collected, processed, disseminated, stored and/or accessed by this information technology (please check each applicable row)	(3) The information relates to: A. DOJ/Component Employees, Contractors, and Detailees; B. Other Federal Government Personnel; C. Members of the Public - US Citizens or Lawful Permanent Residents (USPERs); D. Members of the Public - Non-USPERs	(4) Comments
Military status or other information	X	A, B, C and D	
Employment status, history, or similar information	X	A, B, C and D	
Employment performance ratings or other performance information, e.g., performance improvement plan	X	A, B, C and D	
Certificates	X	C and D	
Legal documents	X	A, B, C and D	
Device identifiers, e.g., mobile devices	X	A, B, C, and D	
Web uniform resource locator(s)	X	C and D	
Foreign activities	X	C and D	
Criminal records information, e.g., criminal history, arrests, criminal charges	X	A, B, C and D	
Juvenile criminal records information			
Civil law enforcement information, e.g., allegations of civil law violations	X	C and D	
Whistleblower, e.g., tip, complaint, or referral	X	C and D	
Grand jury information	X	C and D	Grand jury information collected is limited to authorized individuals.
Information concerning witnesses to criminal matters, e.g., witness statements, witness contact information	X	C and D	Access to this information is limited to authorized individuals.
Procurement/contracting records	X	C and D	
Proprietary or business information	X	C and D	
Location information, including continuous or intermittent location tracking capabilities			
Biometric data:			
- **Photographs or photographic identifiers**	X	C and D	
- **Video containing biometric data**	X	C and D	
- **Fingerprints**			
- **Palm prints**			

(1) General Categories of Information that May Be Personally Identifiable	(2) Information is collected, processed, disseminated, stored and/or accessed by this information technology (please check each applicable row)	(3) The information relates to: A. DOJ/Component Employees, Contractors, and Detailees; B. Other Federal Government Personnel; C. Members of the Public - US Citizens or Lawful Permanent Residents (USPERs); D. Members of the Public - Non-USPERs	(4) Comments
- **Iris image**			
- **Dental profile**			
- **Voice recording/signatures**	X	C and D	
- **Scars, marks, tattoos**	X	C and D	
- **Vascular scan, e.g., palm or finger vein biometric data**			
- **DNA profiles**			
- **Other (specify)**			
System admin/audit data:	X	A	
- **User ID**	X	A	All administrators are provided unique user IDs.
- **User passwords/codes**	X	A	All administrators use unique passwords and Personal Identification Verification (PIV) cards issued in accordance with HSPD-12.
- **IP address**	X	A	IP address information is contained within the system.
- **Date/time of access**	X	A	Access logs with date and time of access are maintained within the system and are generally limited to the user and administrators.
- **Queries run**	X	A	Query runs are maintained within the system and are generally limited to the user.
- **Contents of files**	X	A	Contents of all files are available to administrators.
Other (please list the type of info and describe as completely as possible):	X	C and D	Additional personal information could be collected or received through investigations and litigation.

3.2 Indicate below the Department's source(s) of the information. (Check all that apply.)

Directly from the individual to whom the information pertains:					
In person	X	Hard copy: mail/fax	X	Online	X
Phone	X	Email	X		
Other (specify):					

Government sources:					
Within the Component	X	Other DOJ Components	X	Other federal entities	X
State, local, tribal	X	Foreign (identify and provide the international agreement, memorandum of understanding, or other documented arrangement related to the transfer)	X		
Other (specify):					

Non-government sources:					
Members of the public	X	Public media, Internet	X	Private sector	X
Commercial data brokers	X				
Other (specify):					

Section 4: Information Sharing

4.1 Indicate with whom the Component intends to share the information and how the information will be shared or accessed, such as on a case-by-case basis by manual secure electronic transmission, external user authorized accounts (i.e., direct log-in access), interconnected systems, or electronic bulk transfer.

Information maintained in ATR RelOne may be shared internally within ATR and DOJ with personnel authorized to access the relevant matter, on a role-based, need-to-know basis. Copies of data may be produced externally to courts and to opposing counsel in litigation, and disclosed to expert witnesses and vendors supporting a matter, consistent with applicable court rules, protective orders, and Federal criminal and civil procedures. External sharing occurs in the context of specific investigation or litigation and is governed by the applicable legal process and protective orders.

Recipient	How information will be shared			
	Case-by-case	**Bulk transfer**	**Direct log-in access**	**Explain specifics of the sharing, as well as how these disclosures will support and are compatible with the purposes of the collection.**
Within the Component	X		X	ATR will share information among ATR offices on a case-by-case basis. ATR generally will provide access to data via a RelOne account upon Section Chief/Assistant Chief approval. The requester's access is limited to only the requested data.
DOJ Components	X		X	ATR will share information among other DOJ components on a case-by-case basis. ATR generally will provide access to data via a RelOne account upon Section Chief/Assistant Chief approval. The requester's access is limited to only the requested data.

Recipient	How information will be shared			
	Case-by-case	**Bulk transfer**	**Direct log-in access**	**Explain specifics of the sharing, as well as how these disclosures will support and are compatible with the purposes of the collection.**
Federal entities	X		X	ATR will share information on a case-by-case basis with federal entities with legitimate reasons for access, upon approval of the case manager and the ATR Security staff. Individuals must be cleared by ATR Security prior to access, after which ATR will provide training and grant access to approved/requested data via a RelOne account, utilizing a government furnished equipment (GFE) and/or RSA token through virtual private network (VPN), for direct log-in or using the Justice Enterprise File Sharing System (JEFS)[1]. The requester's access is limited to only the requested data. The requester's access is maintained until termination is directed by the legal staff, or until the end of the case.

[1] JEFS is covered by separate privacy documentation available here: https://www.justice.gov/media/1169496/dl?inline.

Recipient	How information will be shared			
	Case-by-case	**Bulk transfer**	**Direct log-in access**	**Explain specifics of the sharing, as well as how these disclosures will support and are compatible with the purposes of the collection.**
State, local, tribal gov't entities	X		X	ATR will share information on a case-by-case basis with state, local, tribal government entities with legitimate reasons for access, upon approval of the case manager and the ATR Security staff. Individuals must be cleared by ATR Security prior to access, after which ATR will provide training and grant access to approved/requested data via a RelOne account, utilizing a GFE and/or RSA token through VPN, for direct log-in or using the JEFS. The requester's access is limited to only the requested data. The requester's access is maintained until termination is directed by the legal staff, or until the end of the case.
Public				
Counsel, parties, witnesses, and possibly courts or other judicial tribunals for litigation purposes		X		ATR will share case documents with the parties and court as required by discovery rules or court orders. Such documents are often provided to opposing parties and courts in bulk, for example, thousands of documents could be provided and received by the parties in a discovery document production.

Recipient	How information will be shared			
	Case-by-case	**Bulk transfer**	**Direct log-in access**	**Explain specifics of the sharing, as well as how these disclosures will support and are compatible with the purposes of the collection.**
Private sector	X		X	ATR will share information on a case-by-case basis with the private sector with legitimate reasons for access, upon approval of the case manager and the ATR Security staff. Individuals must be cleared by ATR Security prior to access, after which ATR will provide training and grant access to approved/requested data via a RelOne account, utilizing a GFE and/or RSA token through VPN, for direct log-in or using JEFS. The requester's access is limited to only the requested data. The requester's access is maintained until termination is directed by the legal staff, or until the end of the case.

Recipient	How information will be shared			
	Case-by-case	**Bulk transfer**	**Direct log-in access**	**Explain specifics of the sharing, as well as how these disclosures will support and are compatible with the purposes of the collection.**
Foreign governments	X		X	ATR will share information on a case-by-case basis with foreign governments with legitimate reasons for access, upon approval of the case manager and the ATR Security staff. Individuals must be cleared by ATR Security prior to access, after which ATR will provide training and grant access to approved/requested data via a RelOne account, utilizing a GFE and/or RSA token through VPN, for direct log-in. The requester's access is limited to only the requested data. Foreign governments with read access to ATR RelOne are litigating partners in criminal or civil matters. The requester's access is maintained until termination is directed by the legal staff, or until the end of the case.
Foreign entities				
Other (specify):				

4.2 If the information will be released to the public for "Open Data" purposes, e.g., on data.gov (a clearinghouse for data from the Executive Branch of the federal government), and/or for research or statistical analysis purposes, explain whether—and, if so, how—the information will be de-identified, aggregated, or otherwise privacy protected.

ATR provides only statistics and case filings to the "Open Data" site (www.data.gov). ATR's public case filings may properly contain PII.

Section 5: Notice, Consent, Access, and Amendment

5.1 What kind of notice, if any, will be provided to individuals informing them about the collection, use, sharing or other processing of their PII, e.g., a Privacy Act § 552a(e)(3) notice? Will a System of Records Notice (SORN) be published in the Federal Register providing generalized notice to the public? Will any other notices be provided? If no notice is provided to individuals or the general public, please explain.

Individuals involved in investigations and litigation are notified in accordance with Federal criminal and civil procedures and court rules. Individuals may voluntarily submit information that is maintained in ATR RelOne through online forms. ATR's online forms include ATR's Complaint Center, Healthy Competition Complaint Form, Procurement Collusion Strike Force Tip Center, whistleblower report form, and the USDA-DOJ Complaint Portal[2]. The forms include a Privacy Act § 552a(e)(3) notice. In addition, an ATR SORN provides generalized notice to the public.

ATR-006, "Antitrust Management Information System (AMIS) - Monthly Report," 63 Fed. Reg. 8659 (2-20-1998), 66 Fed. Reg. 8425 (1-31-2001), 66 Fed. Reg. 17200 (3-29-2001), 82 FR 24147 (5-25-2017). Exemptions Claimed Pursuant to 5 U.S.C. 552a(k)(2). See 28 C.F.R. § 16.88.

5.2 What, if any, opportunities will there be for individuals to voluntarily participate in the collection, use or dissemination of information in the system, for example, to consent to collection or specific uses of their information? If no opportunities, please explain why.

Individuals involved in investigations and litigation are notified in accordance with Federal criminal and civil procedures and court rules. ATR obtains the majority of the information stored in ATR RelOne through subpoenas, discovery requests, search warrants, civil investigative demands, or second requests under the Hart-Scott-Rodino Antitrust Improvements Act ("HSR Act")[3], and for these mechanisms individuals generally do not have the opportunity to decline to provide the requested information and documents. Certain information may be provided voluntarily.[4] For information collected from public sources, notice is not provided because the information is publicly available.

5.3 What, if any, procedures exist to allow individuals to gain access to information in the system pertaining to them, request amendment or correction of said information, and

---

[2] These portals are covered under existing privacy documentation here: https://www.justice.gov/d9/pages/attachments/2022/06/27/atr_wss_pia_220209_for_publishing.pdf.

[3] The HSR Act, 15 U.S.C. § 18a, requires parties to certain transactions to notify ATR and the Federal Trade Commission of the transaction and to provide certain documents, and it permits the agencies to make a request for additional information and documents (a "second request").

[4] For example, during the initial waiting period of an ATR investigation under the HSR Act, ATR typically requests and parties typically provide the voluntarily submission of certain information and documents.

receive notification of these procedures (e.g., Freedom of Information Act or Privacy Act procedures)? If no procedures exist, please explain why.

ATR's Privacy Program Plan captures policy and procedures to ensure compliance with Federal and Department FOIA guidelines regarding requests for information or amendment, to the extent the information is in a system of records and no exemption exists. All such requests are submitted to the ATR's FOIA/Privacy Act Unit (https://www.justice.gov/atr/antitrust-foia) for processing and response.

Section 6: Maintenance of Privacy and Security Controls

6.1 The Department uses administrative, technical, and physical controls to protect information. Indicate the controls below. (Check all that apply).

X	**The information is secured in accordance with Federal Information Security Modernization Act (FISMA) requirements, including development of written security and privacy risk assessments pursuant to National Institute of Standards and Technology (NIST) guidelines, the development and implementation of privacy controls and an assessment of the efficacy of applicable privacy controls. Provide date of most recent Authorization to Operate (ATO) (if the system operates under an Authorization to Use (ATU) or other authorization mechanism, provide related details wherever an ATO is referenced):** ATO Awarded: 9/26/2025 **If an ATO has not been completed, but is underway, provide status or expected completion date:** **Unless such information is sensitive and release of the information could pose risks to the Component, summarize any outstanding plans of actions and milestones (POAMs) for any privacy controls resulting from the ATO process or risk assessment and provide a link to the applicable POAM documentation:** There are no outstanding POA&Ms associated with privacy controls. All controls have been assessed and satisfied successfully with appropriate supportive artifacts and comments.
	This system is not subject to the ATO processes and/or it is unclear whether NIST privacy controls have been implemented and assessed. Please explain:
X	**This information or information system has been assigned a security category as defined in Federal Information Processing Standards (FIPS) Publication 199, Standards for Security Categorization of Federal Information, and Information Systems, based on the information it contains and consistent with NIST SP 800-60 v.2 rev. 1, Guide for Mapping Types of Information and Information Systems to Security Categories: Appendices. Specify and provide a high-level summary of the justification, which may be detailed in the system security and privacy plan:**

	RelOne is categorized Moderate under FIPS 199 - Confidentiality, Integrity, and Availability each at moderate. Per NIST SP 800-60 V.1, rev.1 mapping, RelOne processes ATR litigation/eDiscovery information, including PII and sensitive investigative material where unauthorized disclosure or loss of integrity would have a serious/adverse effect on operations and individuals. This aligns with RelOne's FedRamp moderate authorization of record. Full justification is detailed in the SSP.
X	**Monitoring, testing, or evaluation has been undertaken to safeguard the information and prevent its misuse. Specify:** ATR SaaS has completed all required security and functional testing and evaluation in accordance with Department IT development procedures. Additionally, the system has undergone a full security assessment in accordance with the DOJ Security and Privacy Assessment and Authorization Handbook.
X	**Auditing procedures are in place to ensure compliance with security and privacy standards. Explain how often system logs are reviewed or auditing procedures conducted:** System activity is subject to audit review. ATR maintains a documented monthly audit-review procedure over RelOne audit records as a manual compensating control; audit records support detection of unauthorized access and role-based access review.
X	**Contractors that have access to the system are subject to information security, privacy and other provisions in their contract binding them under the Privacy Act, other applicable laws, and as required by DOJ policy**. Pursuant to Department policy, contractors are generally required in their contracts to comply with the Privacy Act and other applicable laws. All contractors granted access to ATR SaaS RelOne are required to sign the DOJ General and/or Privileged Rules of Behavior, as determined by their role.
X	**Each Component is required to implement foundational privacy-related training for all Component personnel, including employees, interns, and contractors, when personnel on-board and to implement refresher privacy training annually. Indicate whether there is additional training specific to this system, and if so, please describe:** All ATR SaaS RelOne users are subject to onboarding training that includes computer security awareness and privacy training, which is an annual requirement thereafter. Additional cloud application-level training is offered periodically, as needed for particular functions or users.

6.2 Explain key privacy and security administrative, technical, or physical controls that are designed to minimize privacy risks. For example, how are access controls being utilized to reduce the risk of unauthorized access and disclosure, what types of controls will protect PII in transmission, and how will regular auditing of role-based access be used to detect possible unauthorized access?

All ATR SaaS RelOne users are required to use multi-factor authentication or unique username and passwords to access their ATR accounts. Data access is highly restrictive; users require formal approval and authorization to access information on a case-by-case

basis. Users can access only data for which they are authorized. All users are required to undergo training and sign formal Rules of Behavior prior to being granted access to the ATR SaaS RelOne cloud data.

6.3 Indicate how long the information will be retained to accomplish the intended purpose, and how it will be disposed of at the end of the retention period. (Reference the applicable retention schedule approved by the National Archives and Records Administration, if available.) If the project involves artificial intelligence and/or machine learning, indicate if the information is used for training AI models, and if so, how this will impact data retention and disposition.

Information is retained and disposed of in accordance with Directive ATR 2710.1, "Procedures for Handling Division Documents and Information," consistent with National Archives and Records Administration regulations and records schedules. Data is retained for as long as the matter remains open or until document holds are released and may only be deleted by ATR Internal System Administrators. Material that is not a Federal record or that has completed its retention period is often destroyed or returned to the submitting party. With respect to artificial intelligence: RelOne's AI features operate on case documents and case-related data to generate analyses and recommendations for review by legal professionals. The generative AI capability (Relativity aiR) is built on Microsoft Azure OpenAI services. AI inputs and outputs, including prompt-and-response histories, are retained within the case environment and follow the same retention and disposition requirements as the underlying case data under ATR 2710.1. ATR case data processed through RelOne's generative AI capability (Relativity aiR) is not used to train or fine-tune the underlying foundation models. Consistent with the Azure OpenAI service terms, prompt-and-response data is retained soley within ATR's case environment, is not shared with OpenAI, and follows the same retention and follows the same retention and disposition requirements as the underlying case data under ATR 2710.1.

Section 7: Privacy Act

7.1 Indicate whether information related to U.S. citizens or aliens lawfully admitted for permanent residence will be retrieved by a personal identifier (i.e., indicate whether information maintained by this information technology will qualify as "records" maintained in a "system of records," as defined in the Privacy Act of 1974, as amended).

_____ No. ____X__ Yes.

7.2 Please cite and provide a link (if possible) to existing SORNs that cover the records, and/or explain if a new SORN is being published:

ATR-006, "Antitrust Management Information System (AMIS) - Monthly Report," 63 Fed. Reg. 8659 (2-20-1998), 66 Fed. Reg. 8425 (1-31-2001), 66 Fed. Reg. 17200 (3-29-2001), 82 FR

24147 (5-25-2017). Exemptions Claimed Pursuant to 5 U.S.C. 552a(k)(2). See 28 C.F.R. § 16.88.

Section 8: Privacy Risks and Mitigation

When considering the proposed use of the information, its purpose, and the benefit to the Department of the collection and use of this information, what privacy risks are associated with the collection, use, access, dissemination, and maintenance of the information and how are those risks being mitigated? For projects involving the use of artificial intelligence and/or machine learning, identify the privacy risks uniquely associated with the use of AI/ML, and how those risks are being mitigated, for example the risk of output inaccuracies and mitigations in the form of testing, continuous monitoring, training, secondary review, etc.

Note: When answering this question, please specifically address privacy risks and mitigation measures in light of, among other things, the following:

- ***Specific information being collected and data minimization strategies, including decisions made to collect fewer data types and/or minimizing the length of time the information will be retained (in accordance with applicable record retention schedules),***
- ***Sources of the information,***
- ***Type of technology employed (e.g. AI/ML),***
- ***Specific uses or sharing,***
- ***Privacy notices to individuals, and***
- ***Decisions concerning security and privacy administrative, technical, and physical controls over the information.***

The privacy risks associated with information in ATR SaaS RelOne relate primarily to the loss of confidentiality, integrity, and availability of sensitive data, including personal information collected for investigations and litigation. Unauthorized access to this data could result in improper disclosure, alteration, or destruction of case material. Because ATR's collections are broad and may implicate nearly any category of PII, the volume and sensitivity of the data are themselves risk factors.

These risks are mitigated through data minimization consistent with ATR's mission and applicable retention schedules; role- and group-based access controls enforcing least privilege at the instance, workspace, and object levels; the customer lockbox feature restricting CSP personnel access; multi-factor authentication; encryption of data at rest and in transit; dedicated, segregated instance storage; network allow-listing; mandatory privacy and security training and Rules of Behavior; and a documented audit-review procedure. SSNs, where present, are encrypted and access-restricted, and are redacted before production where not relevant to the litigation. Generalized notice is provided through SORN ATR-006, and access and amendment requests are handled through ATR's FOIA/Privacy Act Unit.

Use of artificial intelligence introduces additional, distinct privacy risks. Because AI features operate on case data in which PII and confidential business information are intermingled, a data breach could expose sensitive information processed by the AI. The prompt-and-response

histories generated by the generative AI (Relativity aiR) constitute a new store of potentially sensitive data that must be protected and retained consistent with the underlying case data. Generative AI also presents risks of output inaccuracy, over-reliance on AI recommendations without adequate human oversight, algorithmic bias affecting equity in legal outcomes, and — for a system that ingests case documents into prompts — the risk of indirect prompt injection through adversarial crafted content in reviewed documents.

These AI-specific risks are mitigated through mandatory human oversight: all AI-generated analyses and recommendations remain subject to review and approval by qualified legal professionals, and the AI is designed to augment rather than replace human decision-making. The AI components provide explanations and citations to referenced documents so reviewers can verify the basis for automated results. AI inputs and outputs are protected by the same encryption, access controls, and data-handling policies as the underlying case data. Performance metrics are established through regular auditing and testing across diverse case types and document sets to assess accuracy, bias, and effectiveness, and training and reference data are reviewed for balanced representation. ATR should ensure prompt-and-response logs are treated as a sensitive data store within the authorization boundary and that AiR indirect prompt-injection risk is addressed through its security assessment and continuous monitoring.