SPIRION

Accurate Data Discovery, Automated Classification & Remediation

Privacy Impact Assessments: Insights from the GDPR

Scott M. Giordano, Esq., FIP, CISSP
VP, Data Protection, Spirion

Why This Presentation?

The nature of personally identifiable information has changed significantly in the last decade:

- The U.S. Office of Management and Budget (OMB) offers a commonly-used definition of PII:
- [I]nformation which can be used to distinguish or trace an individual's identity, such as their name, social security number, biometric records, etc. alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc.

Executive Office of The President, Office of Management and Budget, *M-07-16, Safeguarding Against and Responding to the Breach of Personally Identifiable Information (2007)*, at 1.

Why This Presentation?

OMB updated this in 2017:

- The PII may range from common data elements such as names, addresses, dates of birth, and places of employment, to identity documents, Social Security numbers (SSNs) or other government-issued identifiers, precise location information, medical history, and biometrics.

Executive Office of The President, Office of Management and Budget, *M-17-12, Preparing for and Responding to a Breach of Personally Identifiable Information (2017)*, at 1.

SPIRION formerly Identity Finder

Why This Presentation?

Under the California Information Practices Act, Gov. Code 1798.3:

(a) The term “personal information” means any information that is maintained by an agency that identifies or describes an individual, including, but not limited to, his or her name, social security number, physical description, home address, home telephone number, education, financial matters, and medical or employment history. It includes statements made by, or attributed to, the individual.

Why This Presentation?

Under the GDPR definition (Art. 4):

‘personal data’ means any information relating to an identified or identifiable natural person (‘data subject’); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;

Why This Presentation?

Under the GDPR definition (Rec. 30):

Natural persons may be associated with online identifiers provided by their devices, applications, tools and protocols, such as internet protocol addresses, cookie identifiers or other identifiers such as radio frequency identification tags. This may leave traces which, in particular when combined with unique identifiers and other information received by the servers, may be used to create profiles of the natural persons and identify them.

Why This Presentation?

Under the California Consumer Privacy Act of 2018 definition:

Under the §1798.140(o)(1) of the Act, “personal information” is defined as “information that identifies, relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household.”

Why This Presentation?

a) Identifiers such as a real name, alias, postal address, unique personal identifier, online identifier Internet Protocol address, email address, account name, social security number, driver's license number, passport number, or other similar identifiers.

Why This Presentation?

b) Any categories of personal information described in §1798.80(e) of the California Civil Code, i.e., any information that identifies, relates to, describes, or is capable of being associated with, a particular individual, including, but not limited to, his or her name, signature, social security number, physical characteristics or description, address, telephone number, passport number, driver's license or state identification card number, insurance policy number, education, employment, employment history, bank account number, credit card number, debit card number, or any other financial information, medical information, or health insurance information.

"Personal information" does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records.

Why This Presentation?

c) Characteristics of protected classifications under California or federal law.

d) Commercial information, including records of personal property, products or services purchased, obtained, or considered, or other purchasing or consuming histories or tendencies.

e) Biometric information.

f) Internet or other electronic network activity information, including, but not limited to, browsing history, search history, and information regarding a consumer's interaction with an Internet Web site, application, or advertisement.

g) Geolocation data.

Why This Presentation?

h) Audio, electronic, visual, thermal, olfactory, or similar information.

i) Professional or employment-related information.

j) Education information, defined as information that is not publicly available personally identifiable information as defined in the Family Educational Rights and Privacy Act (20 U.S.C. section 1232g, 34 C.F.R. Part 99).

k) Inferences drawn from any of the information identified in this subdivision to create a profile about a consumer reflecting the consumer's preferences, characteristics, psychological trends, preferences, predispositions, behavior, attitudes, intelligence, abilities, and aptitudes.

NARA's CUI Registry - Privacy

- Contract Use
- Death Records
- General Privacy
- Genetic Information
- Health Information
- Inspector General Protected
- Military Personnel Records
- Personnel Records
- Student Records

General Privacy

Category Description:	Refers to personal information, or, in some cases, "personally identifiable information," as defined in OMB M-17-12, or "means of identification" as defined in 18 USC 1028(d)(7).
Category Marking:	PRVCY
Banner Format and Marking Notes:	Banner Format: CUI//Category Marking//Limited Dissemination Control Marking Notes: •Category Marking is optional when marking Basic CUI unless required by agency policy. Example: CUI//Limited Dissemination Control •Category Marking preceded by "SP-" is required when marking Specified CUI. Example: CUI//SP-Category Marking//Limited Dissemination Control •Whether CUI is Basic or Specified is determined by the applicable Safeguarding and/or Dissemination Authority for a given instance of CUI. •Separate multiple Category Markings by a single forward slash (/) and list Category Markings alphabetically. Example: CUI//Category Marking A/Category Marking B//Limited Dissemination Control •Category Markings for Specified CUI precede Category Markings for Basic CUI. Example: CUI//SP-Category Marking/Category Marking//Limited Dissemination Control •Separate multiple Limited Dissemination Controls by a single forward slash (/). Example: CUI//Category Marking//Limited Dissemination Control/Limited Dissemination Control •Reference 32 CFR 2002.20, CUI Marking Handbook, Limited Dissemination Controls and individual agency policy for additional and specific marking guidelines.

Why PIAs/DPIAs?

A little personal data goes a long way:

- 95% of Americans can be identified by name from just four time/date/location points.
- In 2013, researcher Raquel Hill was able to identify 97 percent of the anonymous participants in Alfred Kinsey's sex research data from the 1930s and 40s.
- In 2008, Netflix published 10 million movie rankings by 500,000 anonymized customers, as part of a challenge for people to come up with better recommendation systems than the one the company was using at that time. Researchers were able to de-anonymize people by comparing rankings and time stamps with public rankings and time stamps in the Internet Movie Database.

From: Bruce Schneier, *Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World*

Where did the DPIA come from?

GDPR Article 35

Data protection impact assessment

Where a type of processing in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data.

So, What are "rights and freedoms"?

"[T]he rights and freedoms" of data subjects primarily concerns the rights to data protection and privacy but may also involve other fundamental rights such as freedom of speech, freedom of thought, freedom of movement, prohibition of discrimination, right to liberty, conscience and religion.

And, Just What is a "High Risk" Process?

No definition, just some examples:

(a) a systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person;

(b) processing on a large scale of special categories of data referred to in Article 9(1), or of personal data relating to criminal convictions and offences referred to in Article 10; or

(c) a systematic monitoring of a publicly accessible area on a large scale.

More on “High Risk”

Evaluation that produces legal effects/significant effects:

- Loss of entitled to a particular social benefit conferred by law, such as child or housing benefit;
- Refusal of entry at the border;
- Being subjected to increased security measures or surveillance;
- Being refused employment or access to goods or services (e.g. Insurance, credit, housing);
- Being charged more for goods or services than he or she would otherwise be charged;
- Prevents exercise of rights under contract, using a service or contract;
- Affects a person’s legal status or their legal rights.

More on “High Risk”

Evaluation that produces legal effects/significant effects:

- Damage, interference, loss or distress to individuals health or well being;
- Affects, or is likely to affect, individuals’ financial or economic status or circumstances;
- Causes, or is likely to cause individuals to change their behaviour in a significant way;

More on “High Risk”

Examples of large-scale processing include:

- A hospital (but not an individual doctor) processing patient data;
- Tracking individuals using a city’s public transport system;
- A supermarket chain tracking real-time location of its customers;
- An insurance company or bank processing customer data;
- A search engine processing data for behavioural advertising; or
- A telephone or internet service provider processing user data.

What the Irish DPC Thinks is "High Risk"

The Data Protection Commissioner of Ireland is proposing that a DPIA is required where an organisation is planning to:

- Use personal data on a large-scale for a purpose(s) other than that for which it was initially collected pursuant to Article 6(4) of the GDPR ;
- Profile vulnerable persons including children to target marketing or online services at such persons;
- Use profiling or special category data to determine access to services;
- Monitor, track, or observe individuals' location or behaviour;
- Profile individuals on a large-scale;

What the Irish DPC Thinks is "High Risk"

- Process biometric data to identify an individual;
- Process genetic data;
- Indirectly source personal data where GDPR transparency requirements are not being met;
- Combine, link or cross-reference separate datasets where such linking contributes to profiling or behavioural analysis of individuals;
- Process personal data based on legislative measure under the Data Protection Act 2018 where suitable and specific measures are required to safeguard the fundamental rights and freedoms of individuals;
- Further process personal data for archiving purposes in the public interest, scientific or historical research or statistical purposes.

Compare: U.S. Privacy Impact Assessment (PIA)

Section 208 of the E-Government Act of 2002:

Privacy Impact Assessment (PIA) is an analysis of how information is handled:

(i) to ensure handling conforms to applicable legal, regulatory, and policy requirements regarding privacy,

(ii) to determine the risks and effects of collecting, maintaining and disseminating information in identifiable form in an electronic information system, and

(iii) to examine and evaluate protections and alternative processes for handling information to mitigate potential privacy risks.

When should a PIA be conducted?

The E-Government Act requires agencies to conduct a PIA before:

- Developing or procuring IT systems or projects that collect, maintain or disseminate information in identifiable form from or about members of the public, or
- Initiating…a new electronic collection of information in identifiable form for 10 or more persons (excluding agencies, instrumentalities or employees of the federal government).

From: *M-03-22, OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002*

PIA Examples from OMB M-03-22:

In general, PIAs are required to be performed and updated as necessary where a system change creates new privacy risks. For example:

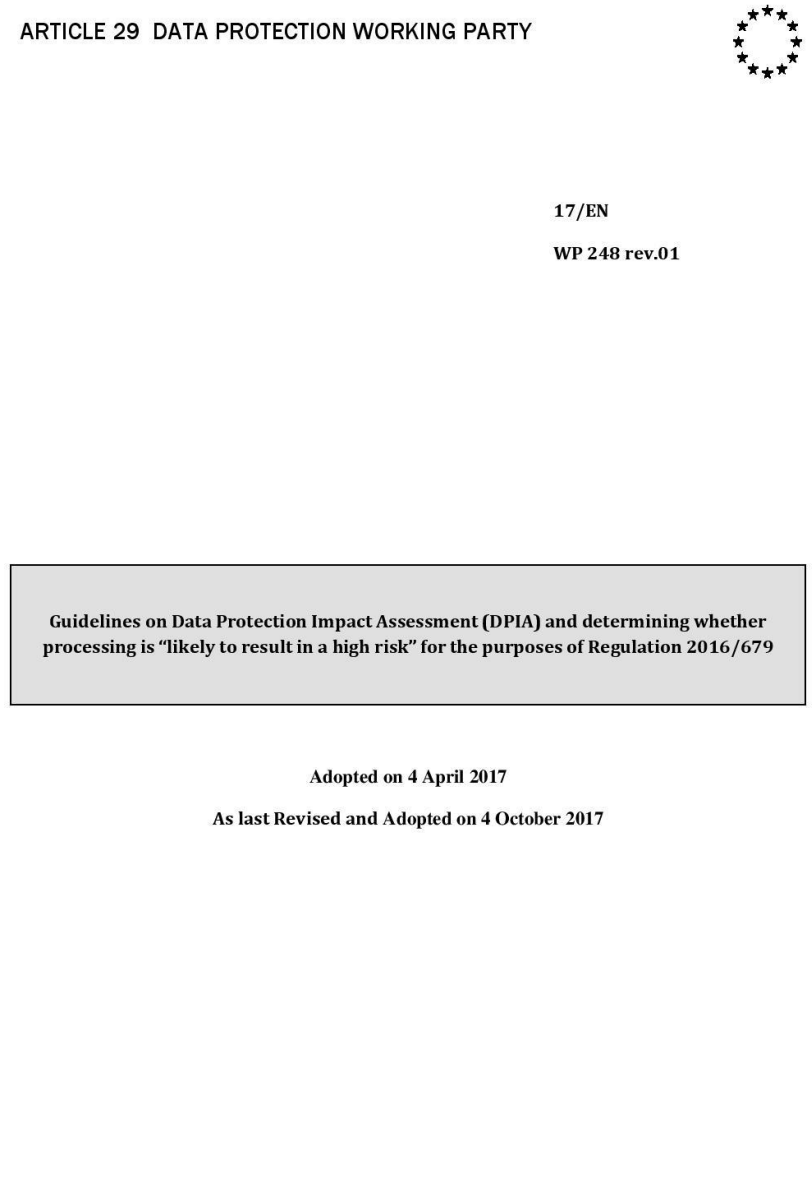
- **Conversions** - when converting paper-based records to electronic systems;
- **Anonymous to Non-Anonymous** - when functions applied to an existing information collection change anonymous information into information in identifiable form;
- **Significant System Management Changes** - when new uses of an existing IT system, including application of new technologies, significantly change how information in identifiable form is managed in the system:
- **New Public Access** - when user-authenticating technology (e.g., password, digital certificate, biometric) is newly applied to an electronic information system accessed by members of the public;

PIA Examples from OMB M-03-22:

- **Commercial Sources** - when agencies systematically incorporate into existing information systems databases of information in identifiable form purchased or obtained from commercial or public sources. (Merely querying such a source on an ad hoc basis using existing technology does not trigger the PIA requirement);
- **New Interagency Uses** - when agencies work together on shared functions involving significant new uses or exchanges of information in identifiable form, such as the cross-cutting E-Government initiatives; in such cases, the lead agency should prepare the PIA;
- **Internal Flow or Collection** - when alteration of a business process results in significant new uses or disclosures of information or incorporation into the system of additional items of information in identifiable form:
- **Alteration in Character of Data** - when new information in identifiable form added to a collection raises the risks to personal privacy (for example, the addition of health or financial information)

Threshold Analysis – the EU View

1. Evaluation or scoring
2. Automated decision making with legal effects
3. Systematic monitoring
4. Sensitive data
5. Data processed on a large scale
6. Matching or combining datasets
7. Data concerning vulnerable data subjects
8. New/innovative technology
9. Prevents a right or using a service or contract



ARTICLE 29 DATA PROTECTION WORKING PARTY

17/EN

WP 248 rev.01

Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679

Adopted on 4 April 2017

As last Revised and Adopted on 4 October 2017

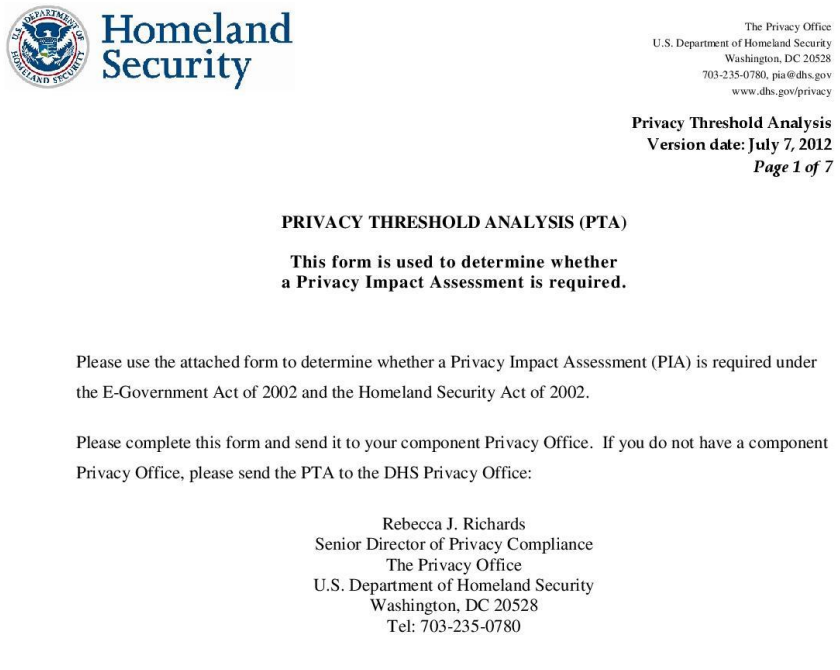
This Working Party was set up under Article 29 of Directive 95/46/EC. It is an independent European advisory body on data protection and privacy. Its tasks are described in Article 30 of Directive 95/46/EC and Article 15 of Directive 2002/58/EC.

The secretariat is provided by Directorate C (Fundamental Rights and Union Citizenship) of the European Commission, Directorate General Justice, B-1049 Brussels, Belgium, Office No MO-59 03/075.

Website: http://ec.europa.eu/justice/data-protection/index_en.htm

Threshold Analysis – the U.S. (DHS) View

1. Project description
2. Project or program status
3. From whom?
    a. DHS Employees
    b. Contractors
    c. The Public
4. What specific information? SSNs?



Homeland Security

The Privacy Office
U.S. Department of Homeland Security
Washington, DC 20528
703-235-0780, pia@dhs.gov
www.dhs.gov/privacy

Privacy Threshold Analysis
Version date: July 7, 2012
Page 1 of 7

PRIVACY THRESHOLD ANALYSIS (PTA)

This form is used to determine whether a Privacy Impact Assessment is required.

Please use the attached form to determine whether a Privacy Impact Assessment (PIA) is required under the E-Government Act of 2002 and the Homeland Security Act of 2002.

Please complete this form and send it to your component Privacy Office. If you do not have a component Privacy Office, please send the PTA to the DHS Privacy Office:

Rebecca J. Richards
Senior Director of Privacy Compliance
The Privacy Office
U.S. Department of Homeland Security
Washington, DC 20528
Tel: 703-235-0780

PIA@dhs.gov

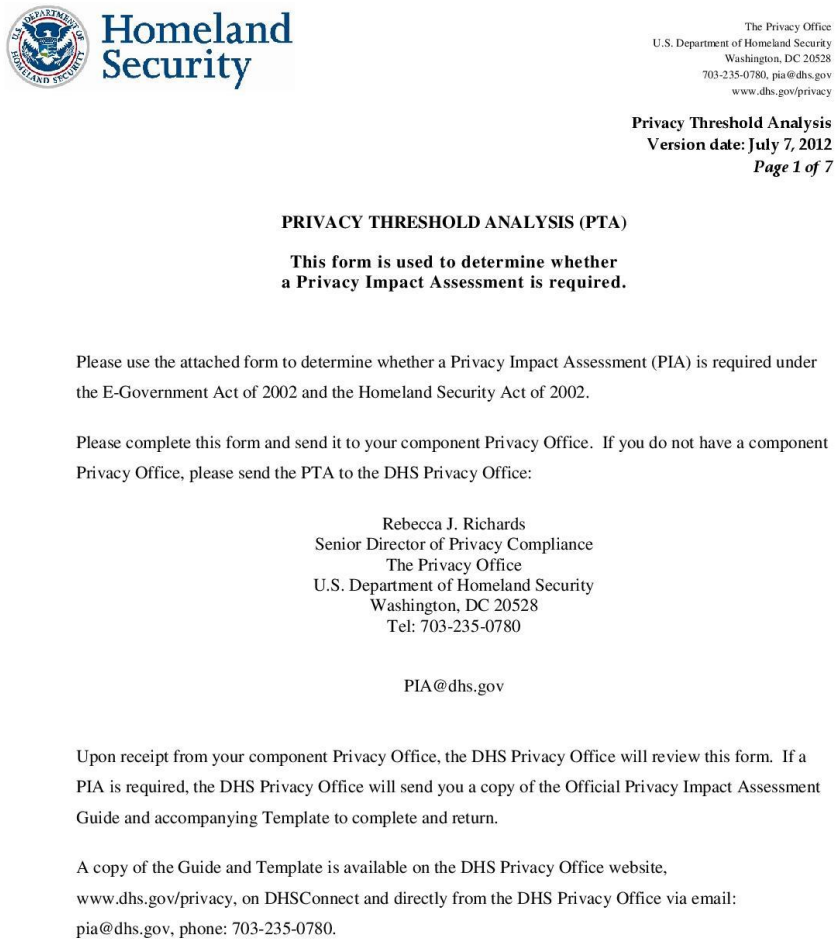
Upon receipt from your component Privacy Office, the DHS Privacy Office will review this form. If a PIA is required, the DHS Privacy Office will send you a copy of the Official Privacy Impact Assessment Guide and accompanying Template to complete and return.

A copy of the Guide and Template is available on the DHS Privacy Office website, www.dhs.gov/privacy, on DHSConnect and directly from the DHS Privacy Office via email: pia@dhs.gov, phone: 703-235-0780.

SPIRION formerly Identity Finder

Threshold Analysis – the U.S. (DHS) View

5. Employ any of the following?:
   a. CCTV, Sharepoint-as-a-Service
   b. Social Media,
   c. Mobile Application (or GPS),
   d. Web portal
6. Does this project or program connect, receive, or share PII with other DHS programs or systems?
7. Does this project or program connect, receive, or share PII with non DHS partners or systems?



Homeland Security

The Privacy Office
U.S. Department of Homeland Security
Washington, DC 20528
703-235-0780, pia@dhs.gov
www.dhs.gov/privacy

Privacy Threshold Analysis
Version date: July 7, 2012
Page 1 of 7

PRIVACY THRESHOLD ANALYSIS (PTA)

This form is used to determine whether a Privacy Impact Assessment is required.

Please use the attached form to determine whether a Privacy Impact Assessment (PIA) is required under the E-Government Act of 2002 and the Homeland Security Act of 2002.

Please complete this form and send it to your component Privacy Office. If you do not have a component Privacy Office, please send the PTA to the DHS Privacy Office:

Rebecca J. Richards
Senior Director of Privacy Compliance
The Privacy Office
U.S. Department of Homeland Security
Washington, DC 20528
Tel: 703-235-0780

PIA@dhs.gov

Upon receipt from your component Privacy Office, the DHS Privacy Office will review this form. If a PIA is required, the DHS Privacy Office will send you a copy of the Official Privacy Impact Assessment Guide and accompanying Template to complete and return.

A copy of the Guide and Template is available on the DHS Privacy Office website, www.dhs.gov/privacy, on DHSConnect and directly from the DHS Privacy Office via email: pia@dhs.gov, phone: 703-235-0780.

SPIRION formerly Identity Finder

Recommendations for Getting Started

- Review your data inventory or create one for the application(s) in question.
- Usually done via interviews with business and technical “owners”
- Validate with data discovery

Sample Data Inventory

Process Descriptions							
Nerve Center' Country (dropdown)	Business teams (dropdown)	Business process activity (e.g. recruiting, payroll calculations, payment processing, etc.)	Description, why activity is done (possible highlight if privacy notice or consent required)	Employees, Customers, Candidates, Suppliers (dropdown)	Types of Personal Data include name, address, date of birth, marital status	personal data type (Standard or Sensitive) - sensitive data type include standard personal data fields	Legal basis for processing
Country	Business Unit	Process flow name	Purpose of the processing	Category of Persor	List of data items	Data Type	Legal Basis
United States	IT	MDM Expert	Mobile Device Management (MDM). Mobile device management (MDM) is software that allows IT administrators to control, secure and enforce policies on smartphones, tablets and other endpoints. MDM is a core component of enterprise mobility management (EMM) which also includes mobile application management, identity and access management and enterprise file sync and share. The intent of MDM is to optimize the functionality and security of mobile devices within the enterprise while simultaneously protecting the corporate network.	Employee	IMSI, IMEI, Device ID, ESN	Standard	Legitimate Interest
United States	IT	DLP Master	Data loss prevention; specifically, file centric actions - e.g., copying from a Word document to Yahoo mail or a USB drive. Data loss prevention (DLP) is a strategy for making sure that end users do not send sensitive or critical information outside the corporate network. The term is also used to describe software products that help a network administrator control what data end users can transfer.	Employee	Equipment identifier (laptop, desktop ID or processor serial number), UserID, AD credentials	Standard	Legitimate Interest

Reproduced with permission from Robert Half Legal Consulting

Sample DPIA Intake/Analysis

Part 1—Data Processing Details
System America Contact Name Contact Email Vendor Address *Vendor Data Protection Officer (or Vendor Privacy Contact) Name:* Insert Name
Is the application owner a controller or processer? ☐ Controller/Co-controller ☐ Processor Has the applicable contract been identified and has review been completed? ☐ Yes ☐ Not

Reproduced with permission from Robert Half Legal Consulting

Nature of Inquiry	☐ Material Changes beyond Original Purpose (“secondary purposes”) ☐ Is there a change in risk profile? (for previously assessed process or application) ☐ Have organizational or societal contexts for the processing activity changed? ☐ Certain automated decisions have become more significant? ☐ New categories of data subjects? ☐ New Types of Information Processed? ☐ New data breach not anticipated in residual risk allocation? ☒ Significant Stakeholder Inquiry? ☒ Use of cloud based system for processing personal data? ☐ System not built with Privacy by Design or Default in Mind?

Category of Personal Data: *Note: Collection of any items in red requires completion of Part II below and a Highly-Restricted Security Classification.*	***Information Type***	***Collect***	***Use***	***Internal Sharing***	***External Sharing***
	Name	☒	☒	☒	☒
	Phone Number	☒	☒	☒	☒
	Physical Mailing Address	☒	☒	☒	☒
	Gender	☒	☒	☒	☒
	Date of Birth	☒	☒	☒	☒
	Marital Status	☒	☒	☒	☒
	Family Information	☒	☒	☒	☒
	Email Address	☒	☒	☒	☒
	Title/Position	☒	☒	☒	☒
	Employer	☒	☒	☒	☒
	Mobile ID	☐	☐	☐	☐
	Gov't ID *(SSN/Passport/Driver's License)*	☒	☒	☒	☒
	Financial Account Information	☐	☐	☐	☐
	Credit Card Information	☐	☐	☐	☐
	Physical Description	☐	☐	☐	☐
	Marital Status	☒	☒	☒	☒
	IP Address	☐	☐	☐	☐
	Image/Video	☐	☐	☐	☐
	Income	☒	☒	☒	☒
	Other (list below)	☒	☒	☒	☒
	Resumes/C.V./job application	☒	☒	☒	☒
	Passport (1 country)	☒	☒	☒	☒
		☐	☐	☐	☐
		☐	☐	☐	☐
		☐	☐	☐	☐
		☐	☐	☐	☐
		☐	☐	☐	☐
		☐	☐	☐	☐
	Click or tap here to enter text.				

Article 9 Special Data				
Race/Ethnicity	☐	☐	☐	☐
Religion or Philosophical beliefs	☐	☐	☐	☐
Health/Medical	☐	☐	☐	☐
Trade Union Membership	☐	☐	☐	☒
Sexual Orientation/Sex Life	☐	☐	☐	☐
Political Opinions	☐	☐	☐	☐
Criminal records	☐	☐	☐	☐
Biometrics and/or genetics for the purpose of identifying a natural person	☐	☐	☐	☐

Geo(s) Represented by the Data Processed by Business Application:	Locations (select all th apply):	☒ *USA*	☒ Canada	☒ *EU*	☒ APAC (not China)	☒ *China*
		☒ Latin America	☐ Global	☒ *Middle East or Africa:* (Explain)		
Geo(s) from Which Data Will Be Accessed:	Locations (select all th apply):	☒ *USA*	☒ Canada	☒ *EU*	☒ APAC (not China)	☒ China
		☒ Latin America	☐ Global	☒ *Middle East or Africa* (Explain)		
Descriptions of Internal and External Parties with Whom the Data Will Be Shared:	**Internal** 3 members of IT; all members of HR information systems					
	External: Click or tap here to enter text.					
	Locations (select all th apply):	☐ *USA*	☐ Canada	☐ *EU*	☐ APAC (not China)	☐ *China*
		☐ Latin America	☐ Global	☐ *Middle East or Africa* (Explain)		
	External Entities (including their groups): Apps Associates					
	Locations (select all th apply):	☒ *USA*	☐ Canada	☐ *EU*	☐ APAC (not China)	☐ China
		☐ Latin America	☐ Global	☒ Other: India		
Application Server Location(s):		☒ *USA*	☐ *Canada*	☐ *EU*	☐ *APAC (not China)*	☐ C
	☐ Latin America			☐ *Middle East or Africa:* (Explain)		
Back-up Server Location(s):		☒ *USA*	☐ *Canada*	☐ *EU*	☐ *APAC (not China)*	☐ C
	☐ Latin America			☐ *Middle East or Africa:* (Explain)		
Disaster Recovery Server Location(s):		☒ *USA*	☐ *Canada*	☐ *EU*	☐ *APAC (not China)*	☐ C
	☐ Latin America			☐ *Middle East or Africa:* (Explain)		

Documentation In scope (reviewed)	☐ Project documents such as Project plan, Project initiation document, business case; ☐ Architectures, such as IT and Enterprise architectures; ☐ Requirements documentation, such as functional, technical and non-functional requirements; ☐ Type of data to be generated and its purpose of use; ☐ Contracts with system engineers, IT hosting parties, IT service providers, Installation and servic providers; ☐ System design documentation, such as interface design, communication protocols.

List and Description of Integrations with Other Applications/Portals: *High-level description of the nature (push or pull) and purpose of the integration (Upload diagram, if available)*	None	
Description of Data Being Sent Through Each Integration:	N/A	
Geographic Regions: *Please indicate from which geographies the data will be accessed.*	☐ *USA* ☐ *Canada* ☐ *EU* ☐ *APAC (not China)* ☐ *China* ☐ *Latin America:* (Explain) ☐ *Other:* (Explain)	
Retention Period Associated with the Data:	Other	**If other:** Indefinite
Data Classification:	Choose an item.	
Application Business Sponsor Approval:	**Signed:** **Name/Date:** Click or tap here to enter text.	

Part II—Data Privacy Risk Assessment
Legitimate Interest, Proportionality and Security

Legitimate Interest:
Indicate the reason(s) for the processing (you can pick more than one, if applicable):Source: GDPR Article 35(7)b

- ☐ Consent
- ☒ Contractual obligation
- ☐ Compliance with a legal obligation
- ☐ Vital Interest
- ☐ Public Interest
- ☒ Legitimate Interest

Proportionality:
Is what we are collecting relevant and limited to what is necessary to accomplish the Interests identified above? Source, GDPR Article 35(7)(b)

- ☒ Lawful, fairly and transparently processed
- ☒ Collected for specific, explicit and legitimate purpose (“Purpose Limitation)
- ☒ Adequate, relevant, and limited to what is necessary (“Data Minimization” and “Privacy by Design”)
- ☒ Accurate & kept up to date (“Accuracy”)
- ☐ Kept in a form which permits identification of data subjects for no longer than necessary (“Storage Limitation”)
- ☒ Processed in manner which ensures appropriate security (“Integrity and confidentiality”)
- ☒ Consistent with Article 25 Data Protection by Design and Default Principals?

☐ Yes ☐ No

Subject Rights
What measures have been taken to ensure the rights of data subjects? Source: GDPR Article (35(&)(b)

- ☐ Information provided to the data subject (Articles 12, 13 and 14);
- ☐ Right of access and portability (Articles 15 and 20);
- ☐ Right to rectify, erase, object, restriction of processing (Article 16 to 19 and 21);

- ☒ Processor(s) (Article 28);
- ☒ Safeguards surrounding international transfer(s) (Chapter V);
- ☐ Prior consultation (Article 36).

Risks:
Identify the risks to the rights and freedoms of the individual data subjects (you can pick more than one, if applicable): Source: Article 35(&)(c), Recital 75, Recital 84, Recital 90, Recital 91,

Feared Event

- ☐ Unavailability of legal processes: they do not or no longer exist or work;
- ☐ Change in processing: it deviates from what was originally planned (diversion of the purpose, excessive or unfair collection...);
- ☒ Illegitimate access to personal data: they are known by unauthorized persons;
- ☐ Unwanted change in personal data: they are altered or changed;
- ☐ Disappearance of personal data: they are not or no longer available.
- ☐ Diverting of personal data to other users: they are distributed to people that have no need.

May give rise to (*check all that may apply and highlight the most relevant to the application or process: Per WP 209, each feared impact should be systematically addressed)*):

- ☐ Discrimination
- ☒ Identity theft or fraud
- ☐ Financial loss
- ☐ Damage to the reputation
- ☒ Loss of confidentiality of personal data
- ☐ Unauthorized reversal of pseudonymization (masking)
- ☐ Any other significant economic or social disadvantage (explain: Click or tap here to enter text.)
- ☐ Loss of independence
- ☐ Loss of freedom of speech and thought
- ☐ Loss of equality;
- ☐ Loss of right to liberty
- ☐ Loss of right to conscience and religion
- ☐ Stigmatization;
- ☐ Loss of freedom to move;
- ☐ Interference with private life
- ☐ Manipulation;
- ☐ Loss of Autonomy.
- ☐ Loss of benefit of right or contract

Data subjects might be *unable* to (*check all that may apply*):

- ☐ Exercise their legal rights
- ☒ Stop the processing of their data
- ☐ Access or view their data
- ☐ Receive copies of their data
- ☒ Correct their data
- ☒ Delete their data
- ☒ Restrict transfer of their data
- ☒ Restrict usage of their data
- ☒ Restrict sharing of their data
- ☐ Otherwise *exercise control* over their personal data (*explain:* Click or tap here to enter text.)

Risk Mitigation:
Identify methods used to reduce privacy risks and protect sensitive elements in the data (you can pick more than one, if applicable):

- ☐ Data filtered to reduce processing of unnecessary subsets of data (*explain:* Click or tap here to enter text.)

- ☒ Data *encrypted* (*check all that apply*):
  - ☐ At rest
  - ☒ In transit

- ☐ Data *anonymized* (*check all that apply*):
  - ☐ Noise addition (range added around data to mask exact data)
  - ☐ Substitution (substitute actual data with code words/values)
  - ☐ aggregation (individual data combined with data of other similar individuals on a blind basis)
  - ☐ Differential privacy applied (any third-party recipients receive only anonymized datasets; only client retains any personal data)
  - ☐ Other anonymization (*explain:* Click or tap here to enter text.)

- ☐ Data *pseudonymized* (obscured in some way) (*check all that apply*):
  - ☐ Hash (map data of any size to code of limited size, e.g., each individual name replaced with two-digit number)
  - ☐ Token (certain data components substituted with non-sensitive equivalent, e.g., different age ranges substituted with colors)
  - ☐ Other anonymization (*explain:* Click or tap here to enter text.)

- ☒ Data access controlled (*check all that apply*):
  - ☐ Discretionary access control (access controlled by client business unit data owner identified in part i above)
  - ☐ Mandatory access control (access controlled based on data sensitivity classification)
  - ☒ Role-based access control (access controlled based on group/role of client user)
  - ☐ Other access control (*explain:* Click or tap here to enter text.)

- ☐ Special instructions/training for Client users accessing data (*explain:* Click or tap here to enter text.)

- ☒ Data management (*check all that apply*):
  - ☒ Data kept up to date (e.g., address updated when individual moves)
  - ☐ Data deleted when no longer needed (e.g., deleted at end of project or contract)
  - ☐ Other management (*explain:* Click or tap here to enter text.)

- ☐ Client monitoring and reporting applied (*explain:* Click or tap here to enter text.)

Additional notes/comments: Click or tap here to enter text.
❑

Input from impacted Parties	☐ Have the views of data subjects or their representatives been solicited? ☐ Where the views of the data subject (or representative") differ from the ultimate determination, those reasons must been documented: ☐ Have the views of the Data Protection Officer been solicited?

Part III — Data Privacy Risk Assessment Decision

Risk Assessment Decision:

☐ Risks sufficiently mitigated (*explain:*)

☐ Risks being addressed (*explain:* Technical measures include: Websense/Forcepoint to monitor network traffic, IPSec encryption for VPN tunnels, McAfee can remotely prevent re-boots if a laptop is stolen, AWS security for the System instance. Administrative measures include: monthly security awareness notices, employee privacy policy, information security policy, acceptable use policy, data processing addendum including model contract clauses for Apps Associates)

☐ Risks accepted (*explain:* Click or tap here to enter text.)

☐ Residual risks (Explain): Must notify Supervisory Authority

Additional notes/comments: Click or tap here to enter text.

CISO sign-off by (sign): _____

Name/Date: Click or tap here to enter text.

Legal Counsel sign-off by (sign): _____

Name/Date: Click or tap here to enter text.

SPIRION formerly Identity Finder

What We Learned

Organizations:

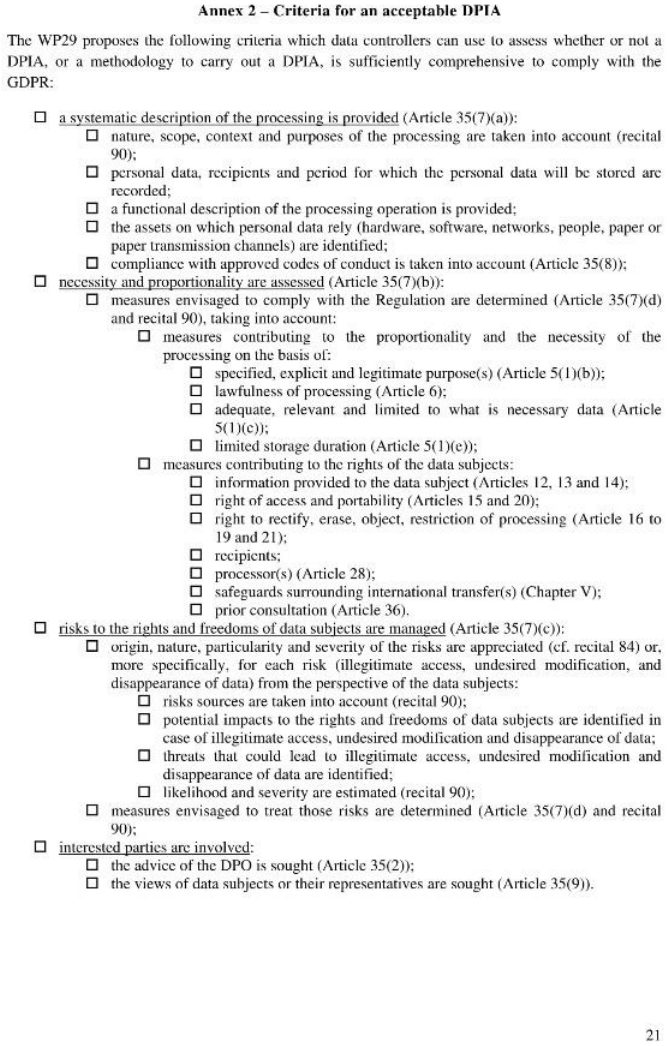
- Do not understand the nature of personal data
- Do not know where personal data lies in their organization's "information ecosystem"
- Do not know with whom data is being shared, inside or outside the organization
- Are not well prepared to legally share personal data
- Are not well prepared to address a data breach
- Are not able to focus team efforts to protect personal data

Summary and Conclusions

- Nature of personal data has expanded significantly, and so have the opportunities for misuse and abuse of that data
- The GDPR introduced the concepts of personal “rights and freedoms” that are impacted by “high risk” processing of that personal data
- The U.S. approach to PIAs – your approach – can benefit greatly from what I call the GDPR’s second opinion on how to conduct those assessments.
- DPIAs tend to dig a level deeper than U.S. PIAs, with an eye to subtle or potentially unforeseen results
- DPIA is ultimately a risk management tool and a living document

Resources

- Art. 29 WP *248 r.01 (Annex 2, at right)*
- *Conducting privacy impact assessments code of practice*, Information Commissioner's Office (ICO), 2014
- Data Protection Commission of Ireland: http://gdprandyou.ie/data-protection-impact-assessments-dpia/
- New ISO standard for DPIAs: *ISO/IEC 29134*



Annex 2 – Criteria for an acceptable DPIA

The WP29 proposes the following criteria which data controllers can use to assess whether or not a DPIA, or a methodology to carry out a DPIA, is sufficiently comprehensive to comply with the GDPR:

- ☐ a systematic description of the processing is provided (Article 35(7)(a)):
  - ☐ nature, scope, context and purposes of the processing are taken into account (recital 90);
  - ☐ personal data, recipients and period for which the personal data will be stored are recorded;
  - ☐ a functional description of the processing operation is provided;
  - ☐ the assets on which personal data rely (hardware, software, networks, people, paper or paper transmission channels) are identified;
  - ☐ compliance with approved codes of conduct is taken into account (Article 35(8));
- ☐ necessity and proportionality are assessed (Article 35(7)(b)):
  - ☐ measures envisaged to comply with the Regulation are determined (Article 35(7)(d) and recital 90), taking into account:
    - ☐ measures contributing to the proportionality and the necessity of the processing on the basis of:
      - ☐ specified, explicit and legitimate purpose(s) (Article 5(1)(b));
      - ☐ lawfulness of processing (Article 6);
      - ☐ adequate, relevant and limited to what is necessary data (Article 5(1)(c));
      - ☐ limited storage duration (Article 5(1)(e));
    - ☐ measures contributing to the rights of the data subjects:
      - ☐ information provided to the data subject (Articles 12, 13 and 14);
      - ☐ right of access and portability (Articles 15 and 20);
      - ☐ right to rectify, erase, object, restriction of processing (Article 16 to 19 and 21);
      - ☐ recipients;
      - ☐ processor(s) (Article 28);
      - ☐ safeguards surrounding international transfer(s) (Chapter V);
      - ☐ prior consultation (Article 36).
- ☐ risks to the rights and freedoms of data subjects are managed (Article 35(7)(c)):
  - ☐ origin, nature, particularity and severity of the risks are appreciated (cf. recital 84) or, more specifically, for each risk (illegitimate access, undesired modification, and disappearance of data) from the perspective of the data subjects:
    - ☐ risks sources are taken into account (recital 90);
    - ☐ potential impacts to the rights and freedoms of data subjects are identified in case of illegitimate access, undesired modification and disappearance of data;
    - ☐ threats that could lead to illegitimate access, undesired modification and disappearance of data are identified;
    - ☐ likelihood and severity are estimated (recital 90);
  - ☐ measures envisaged to treat those risks are determined (Article 35(7)(d) and recital 90);
- ☐ interested parties are involved:
  - ☐ the advice of the DPO is sought (Article 35(2));
  - ☐ the views of data subjects or their representatives are sought (Article 35(9)).

21

SPIRION formerly Identity Finder

Thank you!

Scott M. Giordano, Esq., FIP, CISSP
VP, Data Protection
scott.giordano@spirion.com

What's a Data Protection Impact Assessment (DPIA)?

A DPIA is a process designed to:

- describe the processing;
- assess the necessity and proportionality of a processing; and
- to help manage the risks to the rights and freedoms of natural persons resulting from the processing of personal data.

"In other words, a DPIA is a process for building and demonstrating compliance."

See the Article 29 Working Party document WP248 rev.01

As a practical matter, a DPIA is a risk management/risk mitigation process

Questions to Ask

- Will the project involve the collection of new information about individuals?
- Will the project compel individuals to provide information about themselves?
- Will information about individuals be disclosed to organizations or people who have not previously had routine access to the information?
- Are you using information about individuals for a purpose it is not currently used for, or in a way it is not currently used?
- Does the project involve you using new technology which might be perceived as being privacy intrusive? For example, the use of biometrics or facial recognition.
- Will the project result in you making decisions or taking action against individuals in ways which can have a significant impact on them?
- Is the information about individuals of a kind particularly likely to raise privacy concerns or expectations? For example, health records, criminal records or other information that people would consider to be particularly private.
- Will the project require you to contact individuals in ways which they may find intrusive?

See Conducting privacy impact assessments code of practice, by the U.K. Information Commissioner's Office

DPIA Candidates

- A new IT system for storing and accessing personal data.
- A data sharing initiative where two or more organisations seek to pool or link sets of personal data.
- A proposal to identify people in a particular group or demographic and initiate a course of action.
- Using existing data for a new and unexpected or more intrusive purpose.
- A new surveillance system (especially one which monitors members of the public) or the application of new technology to an existing system (for example adding Automatic number plate recognition capabilities to existing CCTV).
- A new database which consolidates information held by separate parts of an organisation.
- Legislation, policy or strategies which will impact on privacy through the collection of use of information, or through surveillance or other monitoring.

See Conducting privacy impact assessments code of practice, by the U.K. Information Commissioner's Office

Part 1: Collecting Information (1/3)

Information to collect for each application in scope:

- ❑ Application technical owner
- ❑ Application business owner
- ❑ Co-controller or processor?
- ❑ Is there an associated contract?
- ❑ What's the reason for the inquiry?
- ❑ Nature of the processing

Part 1: Collecting Information (2/3)

- Source of the personal data
- Categories of personal data (“regular,” online identifiers, special)
- Data elements (if not already captured)
- Location(s) from which personal data is gathered
- Locations from which is will be accessed
- Server location(s), including replication and backups
- Documentation
- Assets (hardware, software, networks)

Part 1: Collecting Information (3/3)

- Integrations with other systems
- Retention period(s)
- Data classifications(s)

Part 2: Legal Basis, Proportionality, Security

- What's the basis (or bases) for processing?
- How is proportionality addressed?
- How are Data Subject Rights being protected?
- Risks: feared event(s) and potential impacts
- What might Data Subjects not be able to do or what might happen to them as a result?
- Source of the risk?

Part 3: Risk Likelihood and Impact

- Risk likelihood?
- Severity of the potential impact?
- Capabilities of risk sources?
- DPIA required?

Part 4: Risk Mitigation

What risk mitigation measures (administrative and technical) are being applied (or will be)?

- ❑ Encryption
- ❑ Anonymization
- ❑ Pseudonymization
- ❑ Background checks
- ❑ Training
- ❑ Two-Person Integrity
- ❑ Others

Part 5: Risk Assessment Decision and Sign-off

- Risk assessment decision (e.g., risk mitigated, accepted, transferred)
- Residual risks?
- Is there still a high risk?
- Sign-offs by responsible officers (e.g., DPO, CISO, legal counsel)