



Data Protection Risks on a Healthcare Environment

Pablo Segura – Head Data Privacy Argentina & South America
Buenos Aires, Argentina
September 2017

Roadmap



1. Intro: Why there's a data protection regulation?
2. Data Protection Framework: key privacy concepts
 - Personal data; sensitive data; privacy principles, consent; data processing; data transfer; third party processing; crossborder transfers; data security.
3. Data protection risks
4. Key takeaways



Why Data Protection?

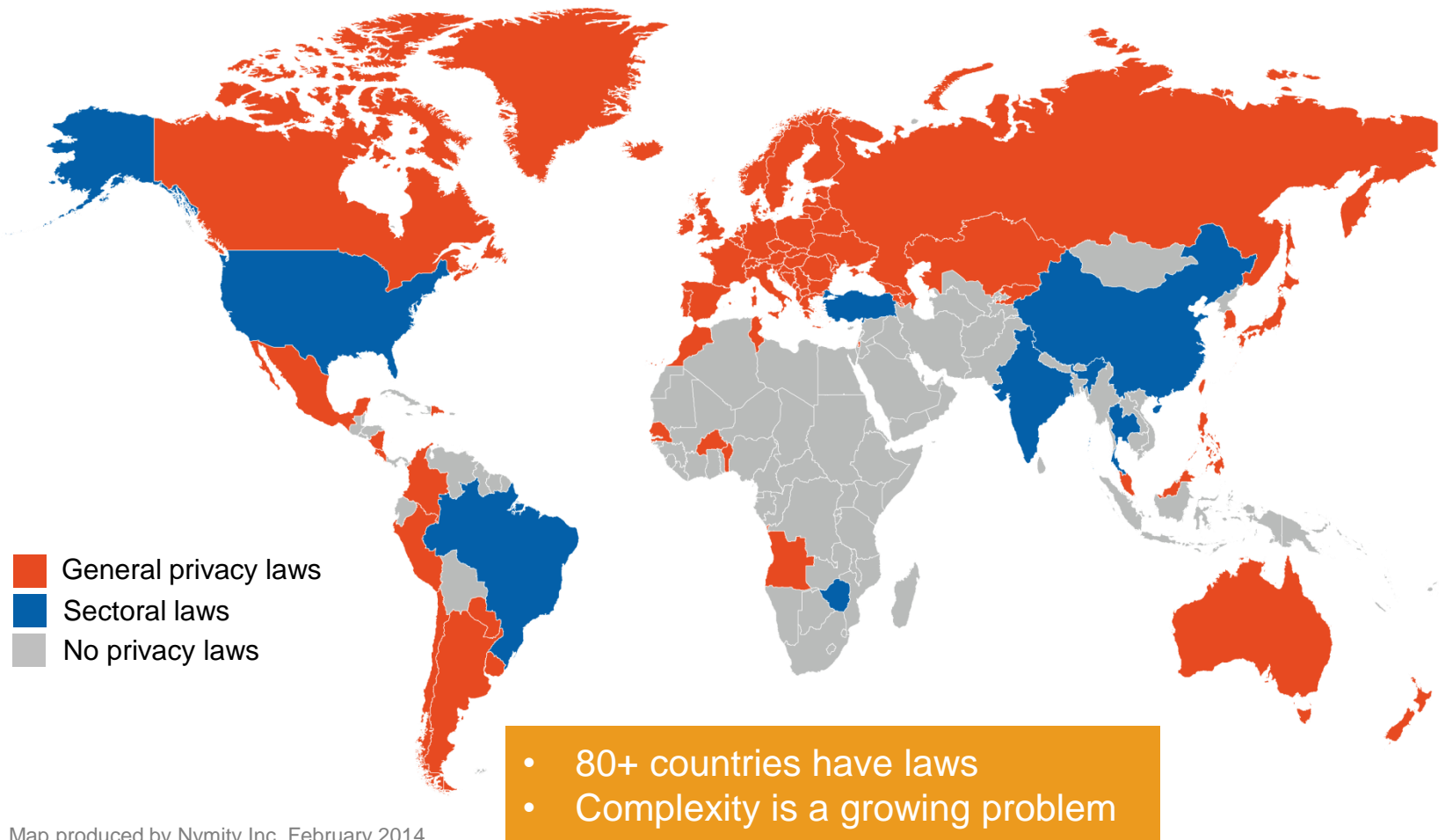


SANDOZ A Novartis
Division

Alcon A Novartis
Division

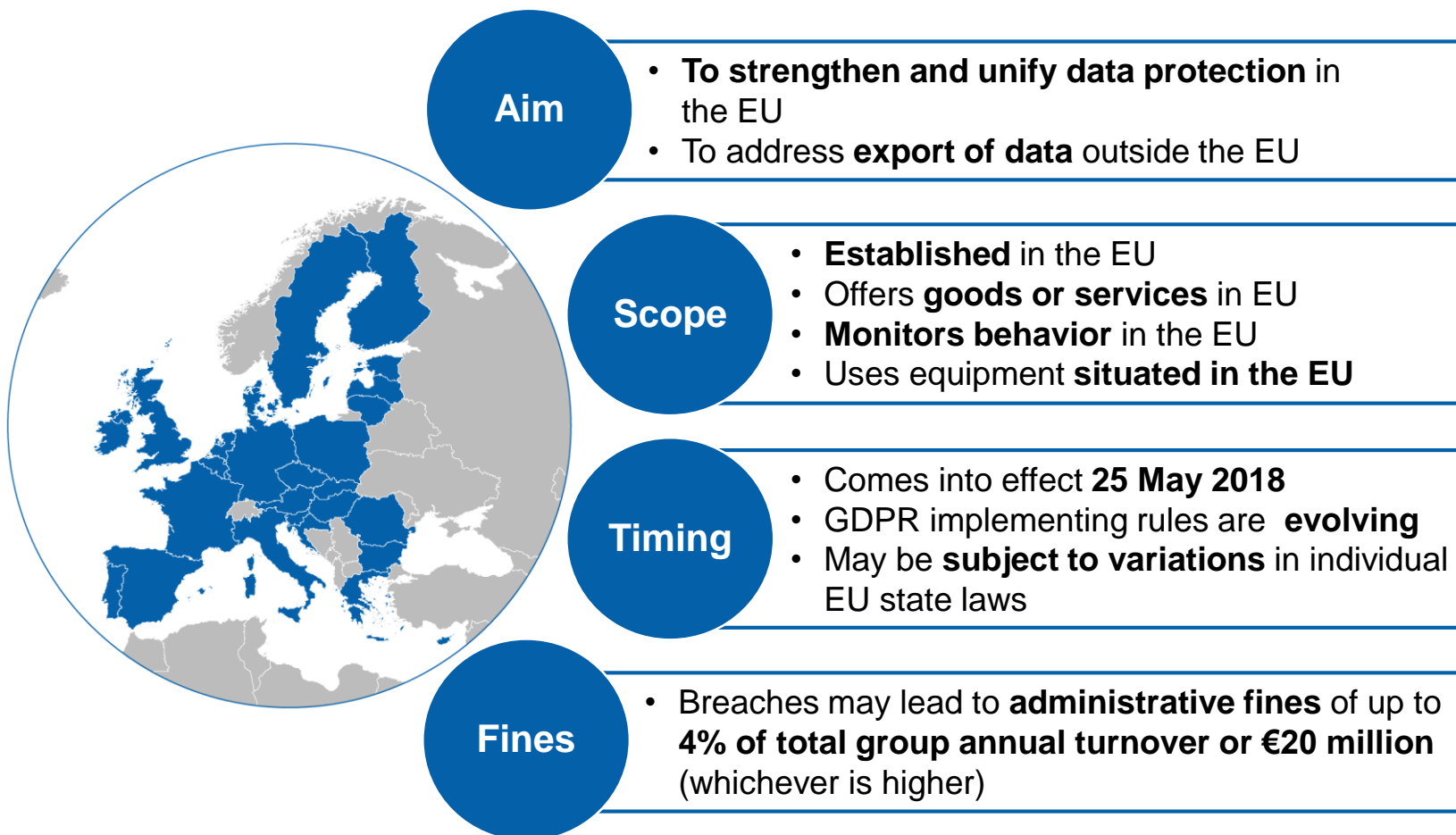
 **NOVARTIS**

What Data Privacy laws are in place around the world?



Map produced by Nymity Inc. February 2014

What changes are coming with GDPR in the EU?



GDPR, General Data Protection Regulation



Data Privacy Framework

SANDOZ A Novartis
Division

Alcon A Novartis
Division

 **NOVARTIS**

What is data protection?

- Data Protection is a **legal right** of each individual to **know and control** the collection, use, and disclosure of their personal information

“For almost every person on Earth, there is at least one fact about them stored in a computer database that an adversary could use to blackmail, discriminate against, harass or steal the identity of him or her ...”

Paul Ohm, 2010



What is personal information?

INFORMATION
RELATING TO A
PERSON



identified



identifiable

The person
could be

natural



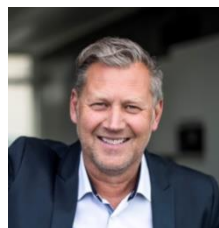
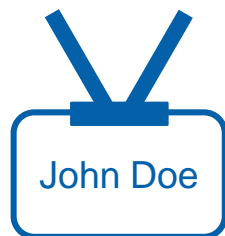
legal



What is personal information?

Direct identifiers

Pieces of information that by themselves identify an individual



Quasi-identifiers

Pieces of information that alone do not identify an individual, but may do so when combined



Health data are considered to be **sensitive** personal information and require a higher level of protection

Sensitive data








SENSITIVE DATA

- philosophic or politic beliefs
- politic parties or trade unions filiation
- religious beliefs
- health information
- sexual orientation
- genetic and biometric data

NON SENSITIVE DATA

- name
- address
- phone number
- profession
- e-mail
- etc.

Principles for the collection and use of personal information

Transparency	Provide clear and detailed notice and obtain consent when required	
Data minimization	Collect only as much data as necessary for the specific purpose	
Purpose limitation	Use data only for the original purpose	1 purpose
Confidentiality	Disclose data for legitimate reasons only	
Access rights	Enable individuals to exercise their right of access, right to rectify and right to be forgotten	
Data quality	Keep data accurate and up-to-date	
Data retention	Retain data only for as long as necessary for the specific purpose	
Data security	Keep data secure through technical and organizational measures	

Consent



- **Express**
 - In writing
 - through any other similar means
- **Informed** (purpose; id of processor; rights; consequences of providing the data; etc.)
- **Exceptions**
 - source of unrestricted public-access
 - data processing by competent authorities
 - lists limited to name, national identity card number, taxing or social security identification, occupation, date of birth, domicile and telephone number
 - contractual, scientific or professional relationship
 - transactions performed by financial entities

What is processing?

Any operation or set of operations performed on personal data



What is data transfer?



- ✓ Transfer means **disclosure** of personal information carried out by any person other than the data subject.
- ✓ Includes transfers among **same group companies** and **third parties** outside group.
- ✓ Disclosure is the **accessibility** of personal information including:
 - Physical transfer to third parties
 - Distribution
 - Publication through manual, electronic or verbal means and
 - Viewing or accessing data (including remote access)

Third party data processing

Controller

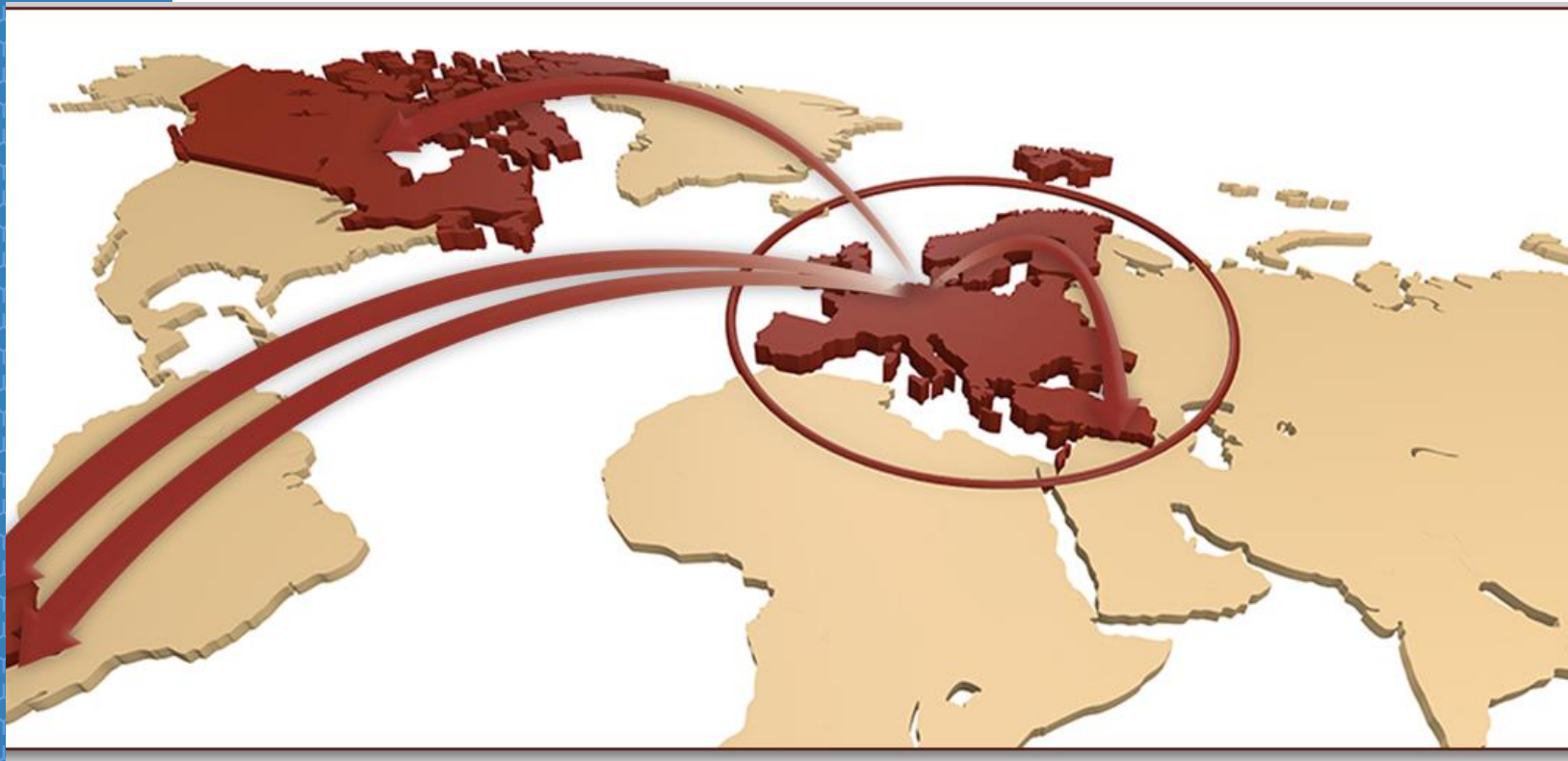
- **Determines the purposes and manner of the processing**
- Remains liable for data protection violations
- Controller must have in place data security measures and ensure protection by third parties processing the data
- Is usually the customer in outsourcing projects

Processor

- **Processes on behalf and under instructions of the Controller**
- Does not determine purposes and means of processing
- Must have in place the technical and organizational measures to ensure data security
- Is usually the supplier in outsourcing projects

Requirements when outsourcing - overview

- **Due diligence of processor:** Supplier must guarantee data security.
 - Vendor assessment, processing agreement, audit
- Parties enter into a **processing agreement** including **key privacy clauses** and a **security compliance plan**.
 - Supplier acts on behalf of and under instructions by controller.
- **Liability:** Controller remains responsible and liable for breaches of applicable laws.
- **Establish policies and procedures for off-shore and outsourcing projects and comply with local laws!**



Cross border data transfers

Cross-border data transfers



Section 12 of Law 25326 (Argentina)

International transfer of data is forbidden to non-adequate countries

Exception: anonymous and encrypted data, consent.

Cross-border data transfers

The DPA enacted Disposition No. 60/15 which:

- approved two model contracts to use to transfer data to “inadequate” countries;
- establishes the need to request authorization to use a different model;
- determined which are the “adequate” countries.



Adequate countries

EU and EEA, SWITZERLAND,
GUERNSEY, JERSEY, ISLE OF
MAN, FAROE ISLANDS, CANADA,
ANDORRA, NEW ZEALAND,
URUGUAY and ISRAEL

Cross-border data transfers from Argentina are restricted

Legal methods for cross-border data transfers out of Argentina to other countries

Adequacy

Template data transfer agreements (Disp. 60 – DNPDP)

Non-template data transfer agreements (with DPA authorization)

Exceptions (e.g., consent)

Binding Corporate Rules (BCR) for intragroup transfers (homologated by DPA)



Data security

Data security

DISP. DNPDP N° 11/06

- **3 LEVELS OF SECURITY:**
 - a. Basic
 - b. Medium
 - c. Critic

In each level, specific security measures should be taken.

Data breaches

- **Loss of storage devices (server, desktop, laptop, mobile device, disk, tape, paper files, USB sticks)**
- **Violations of privacy and information security policies**
- **Unauthorized outside access**
- **Unauthorized internal access**
- **Disclosure of information to an unauthorized person**
- **Accidental destruction or elimination of Personal Data**
- **Loss of equipment (computer, mobile phone)**



What to do?

- ✓ **Is there a mandatory notice to the DPA? (ARG: Disp. DNPDP N° 11/06: keep record of the data breach)**
- ✓ **Establish and comply with data breach procedure**
- ✓ **Immediately involve your DPO**



Identifying DP risks

Data privacy risks

a **risk** is the possibility of an event having a **negative impact** on the company



risk **identification** is key to **managing** and **mitigating** risks.

DP risks assessment

1. Understand

- ✓ What personal information does the organization **collect** and **retain**?
- ✓ What personal information does the organization **need** and **use** in carrying out business?
- ✓ What personal information is **obtained from** or **disclosed** to affiliates or third parties?
- ✓ What is the **impact** of privacy laws and regulations, and/or international privacy requirements, on the organization?
- ✓ How does the organization's business plan **address** the privacy of personal information?



DP risks assessment

Develop a
risks
catalogue



Data Privacy Risks Catalogue	A. Legitimacy of personal data collection
	A1. Inadequate data subject consent (when required)
	A2. No database registration with DPA (when required)
	B. Processing of personal data
	B1. Purpose limitation
	B2. Inadequate minimization and retention
	B3. Inadequate data transfers management
	C. Data subjects rights
	C1. Data subjects rights not handled
	D. Third party processing
	D1. Inadequate vendor assessment / monitoring
	D2. Deficient processing agreement
	E. Cross border data transfers
	E1. Non compliance with legal requirements
	F. Information security
	F1. Inadequate security measures
	F2. Inadequate data breach handling
	G. Data privacy governance
	G1. Inadequate DP management structure and policies
	G2. Deficient employee training

DP risks assessment

2. Implement

- ✓ What **privacy policies** has the organization established for personal data processing?
- ✓ Has the organization **assigned someone** the responsibility for compliance with data privacy?
- ✓ Are **adequate resources** available for developing, implementing, and maintaining a privacy compliance system?
- ✓ How are the policies for managing personal information **communicated** to employees?
- ✓ How are employees with access to personal information **trained** in privacy protection?



DP risks assessment

3. Manage

RISK IDENTIFICATION



CONTROL LEVEL



RISK ASSESSMENT



RISK TREATMENT

Which are the risks and the **consequences** of not meeting the specific privacy objectives?

To what extent have appropriate **control measures** been identified and implemented?

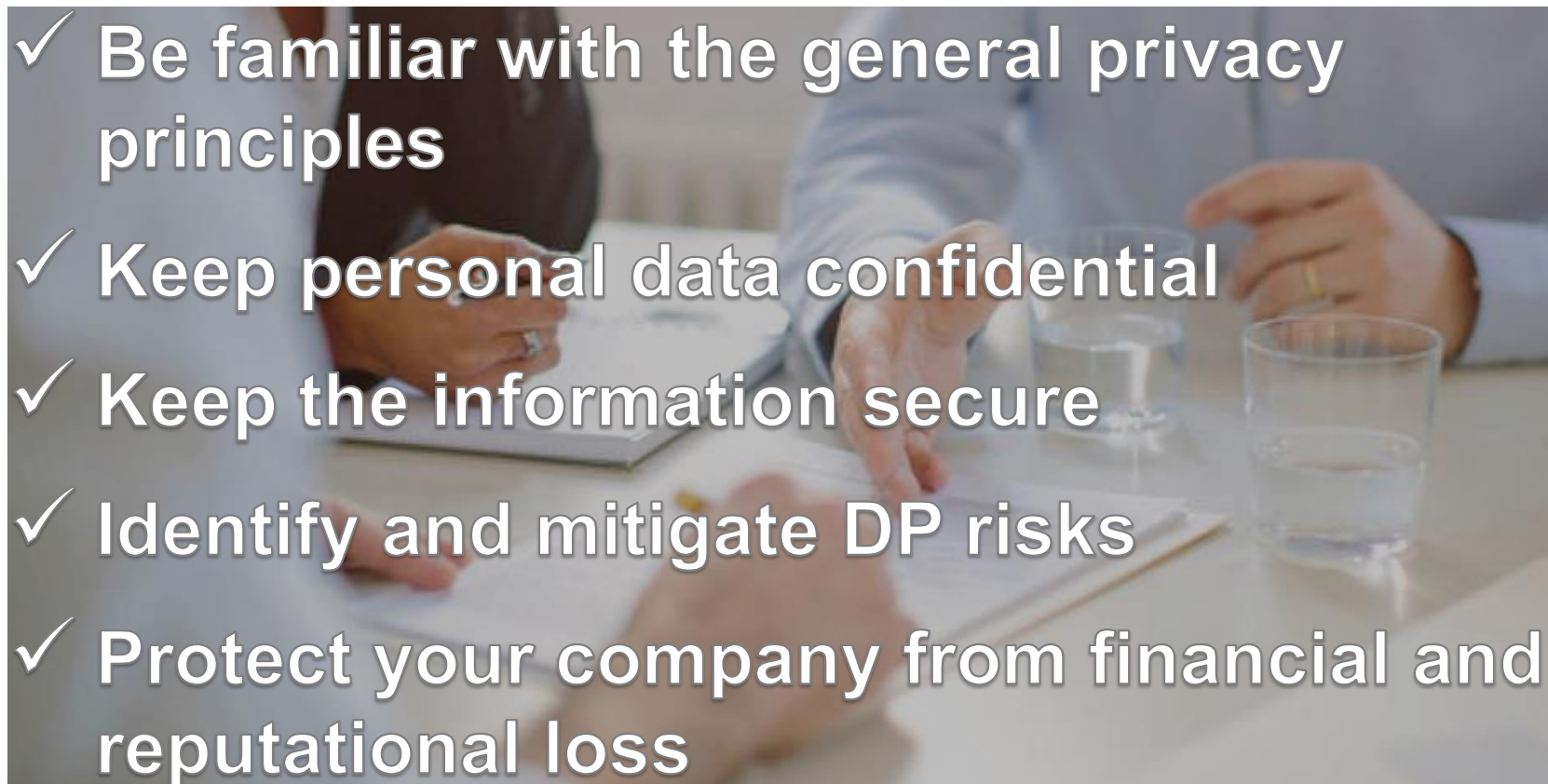
How is the **effectiveness** of the privacy control measures monitored and reported?

What **mitigation activities** are in place to effectively address the risks?



Key Takeaways

Your commitment to data privacy

- 
- ✓ Be familiar with the general privacy principles
 - ✓ Keep personal data confidential
 - ✓ Keep the information secure
 - ✓ Identify and mitigate DP risks
 - ✓ Protect your company from financial and reputational loss



THANKS FOR YOUR ATTENTION

Pablo Segura

Head Data Privacy Argentina & South America

Phone : +54 11 4703 7181

Mobile: +54 9 11 4022 8520

e-mail: pablo.segura@novartis.com