DNS WOMEN
22 MARCH 2021

Australian Reform of Privacy

Holly Raiche, ALAC

Final Report: Topics

The Rise of Platforms

Market Power (and abuse)

Platforms and Advertising

Platforms - Regulatory Frameworks

Platforms and the Media

Commercial relationships and Monetisation

Choice and Quality of News and Journalism

Digital Platforms and Consumers

Harms, from scams, IA and new technology

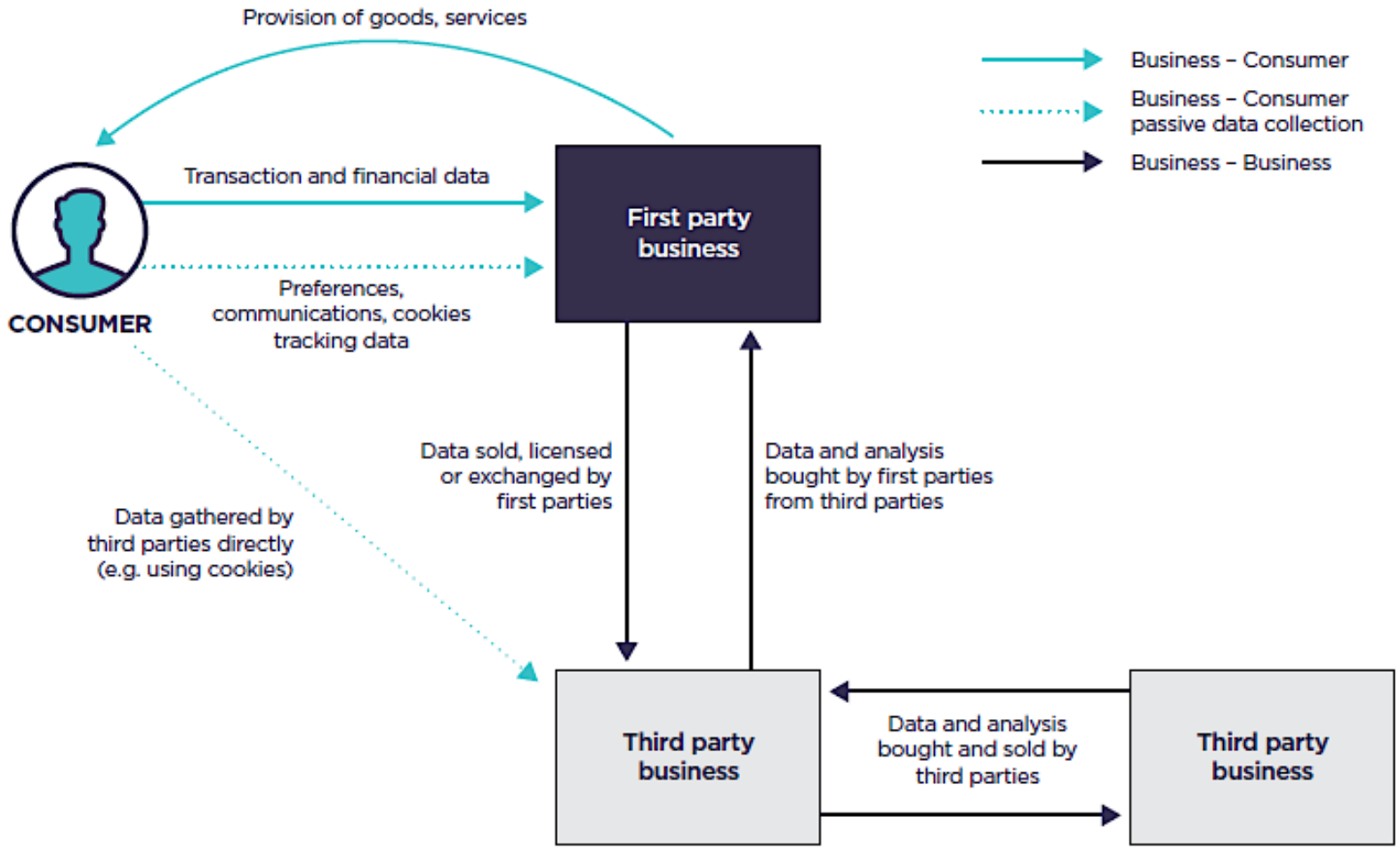
https://www.accc.gov.au/site-search/digital%20platforms%20inquiry

Report's Discussion of Privacy Issues

- Public Awareness of privacy
- Collection of personal data/location data
- Online tracking
- Sharing of data with third parties
- Nature of Consumer consent including bundled consent
- Disclosures in privacy and data policies
- Information Overload, Complexity, Ambiguity, Difficulty of Navigation
- Definition and understandings of Personal Information
- Combining and sharing of data sets
- Extent of Consumer Control/Impact on Consumers

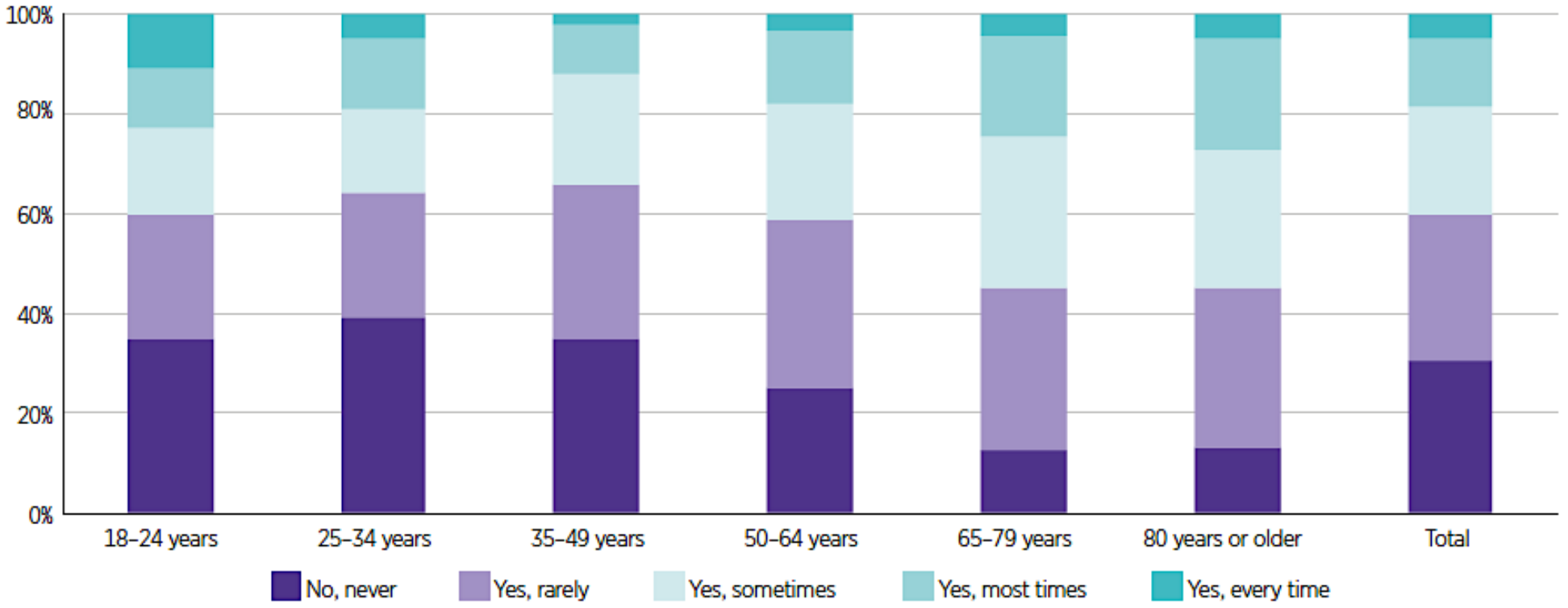
The Data Flows

Figure 7.7: Illustration of data flows between consumers and businesses



Consumer Consent: Do You Read Privacy Policies?

Figure 5.6: How often users read privacy policies[574]



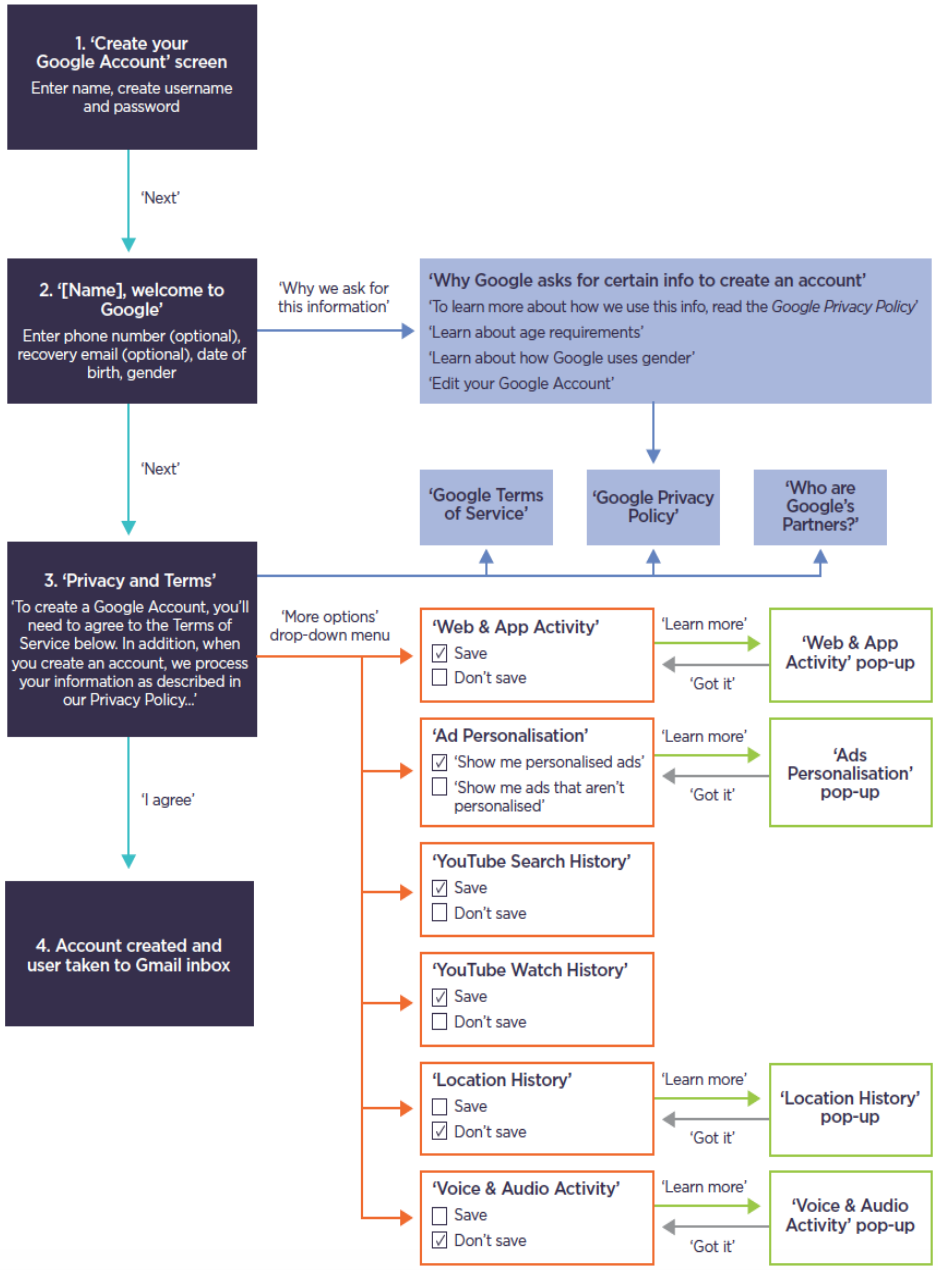
Source: ACCC consumer survey. Q12. Do you normally read all the privacy policy or terms and conditions for an internet site or app?

Complexity of Consenting

Gmail sign-up Flow Chart

Gmail sign-up flow chart

Figure 3: Sign-up process for a new Google Gmail account



Key findings

- In Australia, the collection, use and disclosure of personal information is primarily regulated under privacy laws.
- Strong privacy protections that inform and empower consumers can promote competition, innovation, and the welfare of individual consumers in digital markets.
- The existing Australian regulatory framework for the collection, use and disclosure of user data and personal information does not effectively deter certain data practices that exploit the information asymmetries and bargaining power imbalances between digital platforms and consumers.

ACCC Recommendations on Privacy

- Strengthen Protections in the Privacy Act
  - *Definition of Personal Information (to capture technical data – IP addresses, device identifiers, online identifiers)*
  - *Notification Requirements*
  - *Consent Requirements*
  - *Erasure of Personal Information*
- Broader Reform of Australian Privacy Law
- Privacy Code for Digital Platforms
- Statutory Tort for serious invasion of privacy

The Government's Response:

For 2019/20:

- Review of Social Media Reforms - underway
- Commence Review of the Privacy Act – Announced December 2019

For 2020/21:

- Review of the Privacy Act Underway– until November 2020

  (over 150 submissions received)
- Second Issues Paper expected in 'early 2021'

Questions

Thank you

PROTECTION OF PERSONAL DATA IN THE DIGITAL ENVIRONMENT

Lawyer Romina Florencia Cabrera. UNLP Doctor Candidate. United Nations Order of Merit of Letters. Researcher. Consultant. Teacher.

INTRODUCTION

PRIVACY, RIGHT TO PRIVACY AND ITS IMPACT ON THE DIGITAL AGEIn the so-called Information Society, all the protagonists that make up the same, we are immersed in a technological and interconnected world before never imagined or planned. Training for the correct use of computer tools and the improvement of systems has led to optimizing both technical and human resources, at the service of the digital age.

HUMAN RIGHTS

Human Rights find their foundation in the dignity and worth of the human person. This was established by the Vienna Convention of Treaties.The right to Privacy, Privacy and the protection of personal data (autonomous and independent right, according to the Spanish data protection agency) are fundamental rights, protected by International Treaties and by the National Constitution.

RECOMMENDATIONS ON PROTECTION OF PERSONAL DATA AND HANDLING OF PERSONAL INFORMATION

Prevention is the best security tool for the protection of personal data, and in addition to all government actions or public policies, education acts as the most effective option when it comes to alerting society about good practices in the use of data. network, and inform it about its dangers. Education is the basis of the exercise of freedom in a society, with the self-discipline of its members, as rational beings, in the thought of John Stuart Mill

Observatorio Iberoamericano de Protección de Datos

Iniciativa sobre privacidad, protección de datos y habeas data en Iberoamérica

The Ibero-American Observatory for Data Protection, academic and multidisciplinary in nature, is a legal and technical space where Ibero-American colleagues from different cultures, ethnicities and universities

REGULATIONS IN ARGENTINA

The protection of personal data is guaranteed in our country, through the habeas data action incorporated in article 43, third paragraph, of the National Constitution, at the time of the 1994 Constitutional Reform.Subsequently, Law No. 25,326 on the Protection of Personal Data was enacted, a public order rule that regulates the applicable principles. ARGENTINE LAW complies with the minimum standards established by the European Data Protection Regulation.

ABSTRACT

For the purposes of this law, it is understood by:- Personal data: Information of any kind referring to specific or determinable natural or ideal existence persons.- Sensitive data: Personal data that reveals racial and ethnic origin, political opinions, religious, philosophical or moral convictions, union affiliation and information regarding health or sexual life.- File, register, database or database: Indistinctly, they designate the organized set of personal data that is the object of treatment or processing, electronic or not, whatever the modality of its formation, storage, organization or access.

THANKS!!!!!

UN HONOR Y UN PLACER

Data Protection USA

Karla Valente
March 2021

Principal Protection Legislation

No single data protection legislation in USA - hundreds of laws enacted on federal and state levels serve to protect personal data of U.S. residents.

- **Federal Level** - Federal Trade Commission Act broadly empowers the U.S Federal Trade Commission (FTC) to bring enforcement actions to protect consumers against unfair or deceptive practices and to enforce federal privacy and data protection regulations.

  FTC position - ¨deceptive practices¨ include a company failure to comply with its published privacy promises and its failure to provide adequate security of personal information, in addition to its use of deceptive advertising or marketing methods.

- **State Level** - statutes protect a wide range of privacy rights of individual residents and often differ from one another (e.g. protection of library records, drone surveillance, etc)

Authority Responsible for Data Protection

- No general federal legislation, but several laws sector specific or focus on a particular type of data.
- No plenary data protection regulator
- FTC is very broad and sets tone on federal privacy and data protection issues.
  - Specific Agencies regulate data protection through sectoral laws
  - Department of Health and Human Services, Office of the Controller of the Currency, Federal Communications Commission; Securities and Exchange Commission, COnsumer and Financial Protection Bureau and Department of Commerce

Federal Level Examples

Children Online Privacy Protection Act (COPPA)

- Prohibits collection of any information from a child under age of 13 online from digitally connected devices; requires publication of privacy notices and collection of verifiable parental consent when info is collected.

Video Privacy Protection Act (VPPA)

- Restricts disclosure of rental or sale records of videos or similar audio-visual materials, including online streaming.

Federal Level Examples

HIPAA - Health Insurance Portability and Accountability Act of 1996

- Protects privacy of personal health information
- Carries penalties - from US$100 to US$50,000 per record violation

E-Sign - Electronic Signatures in Global and National Commerce Act

- Describes and validates electronic forms of data, including e-signatures

State Level

- May impose restrictions and obligations on businesses relating to the collection, use, disclosure, security, or retention of certain categories of information (e.g. biometric data, medical records, SSN, financial and tax records etc.)
- Every state has data breach notification that applies to a certain type of personal information about its residents, even if a business does not have a physical presence in a particular state, it must comply when faced with unauthorized access to, or acquisition of, personal information it collects, holds, or processes about that state´s residents.

State Level Examples

California Consumer Privacy Act (CCPA)

- It applies to any organization doing business in California and which has gross revenues in excess of US$25 millions or that has 50,000 of more personal records or that earns ½+ of its revenue from selling personal information.
- Penalties per violation: US$2,500 to US$7,500.

NY Shield Act

- Applies if one holds any personal or private data of any New York resident.
- Penalties for violation: US$20 or US$5,000; up to US$250,000 maximum.

What to Expect in the future?

- Increase in State Privacy Laws.
- Effort in Congress to enact federal data privacy legislation.
  - More non uniform state laws (confusion, overlapping interested, compliance costs for businesses, etc).
  - Help U.S. businesses to better compete on global market.
  - New legislation framework likely to be similar to CCPA and GDPR. Unlikely more restrictive.

Some Global Trends

- **Privacy officer** - Like GDPR requirement, many privacy laws around the world are introducing requirements to have an individual appointed and accountable for privacy.
- **Penalties** - financial penalties for violations of privacy legislation or even for improper breach in handling data, can have monetary and reputational impact
- **Privacy Programs** - organizations are establishing privacy programs (e.g. privacy policies, staff training and awareness, breach management plan, etc).
- **Consent** - consent for collection of personal data including a precise description of the planned use for the data collected.
- **Breach Management and Notification** - documented breach management plan and notification processes

DNS WOMEN
Est. 2009
Connect > Inspire > Thrive

ICANN 70
VIRTUAL COMMUNITY FORUM

DNS WOMEN PANEL on Data Protection

VANDA SCARTEZINI
BRAZILIA LAW

Brazilian Legislation (LGPD)

LGPD

Law nº 13.709, August 14, 2018

Valid from September 18,2020

Sanctions ; August 1st ,2021

ANPD – Data Protection National Agency (in charge of rules of procedures and Sanctions)

Lei Nº 13.853, July 8, 201

Operational from August 26. 2020

Applicability

Art. 3 This **Law applies to any treatment of personal data**, by any legal person, national or international, public or private, regardless of the medium, host country or place where the data is stored - **provided that:**

i. The **treatment** operation is **carried out in the national territory**;
ii. The processing activity aims at offering or **providing goods or services or processing data** from **individuals located in the national territory**;
iii. The **personal data** subject to the treatment have been **collected in the national territory** and the **holder is in the national territory at the time of collection**.

Art. 4 This Law **does not apply** to the processing of personal data:

i. Performed by a natural person for private and non-economic purposes;
ii. Carried out for purposes: **journalistic and artistic / academic** with **general restrictions**
iii. Carried out for the exclusive purposes of: public security / national defense / State security / or investigative activities and prosecution of criminal offenses. Item governed by specific legislation in the **public interest.**
iv. Coming from **outside the national territory** and that are **not** the **subject** of communication, shared use of data or **international data transfer** with another country that provides a degree of protection similar to the LGPD.

Brazilian Law X GDPR

Similarities ✅ & Differences ⛔

- The right to be informed ✅
- The right to access ✅
- The right to rectification ✅
- The right to be forgotten ⛔
- The right to have restricted processing
- The right to data portability ✅
- The right to object ✅
- Controller/Operator and DPO ✅
- The right not to be subject to an automatic decision even if the information is free. ⛔
- Compliance obligation throughout the supply chain ✅
- GDPR has no Harmonization among actors, by the Agency. ⛔

Differences

- **Right to be forgotten -** The LGPD does not provide, but guarantees the holder the right to delete (delete) data (arts, 5, 16 and 18). Our Constitution prohibits anonymity.
- **Right to have restricted processing -** The LGPD does not provide, but it is possible to conclude that the holder has this right. The principle of necessity (art. 6, item III) limits treatment to the minimum necessary to achieve its purpose.
- **Right not to be subject to an automatic decision** - LGPD does not provide, but guarantees the holder the right to request a review (art. 20, caput) and the right to obtain information about the criteria and procedures that guided automated decisions. (art. 20, paragraph 1).
- **Harmonization between actors** – GDPR does not require but a recent EU study shows a possible need.

Other differences & similarities

Territorial coverage

- GDPR and LGPD laws are both GLOBAL

Feedback to the titular (owner personal data)

- GDPR : within 1 month
- LGPD : 15 days

DPO – Data Protection Officer

- Mandatory for Public Organisations + Private with large personal data treatment
- Mandatory for all – the Agency is studying to restrict the universe of obligation

Time to report data leaks to Agency

- Within 72 hours
- The Agency

Controller X Operator relationship

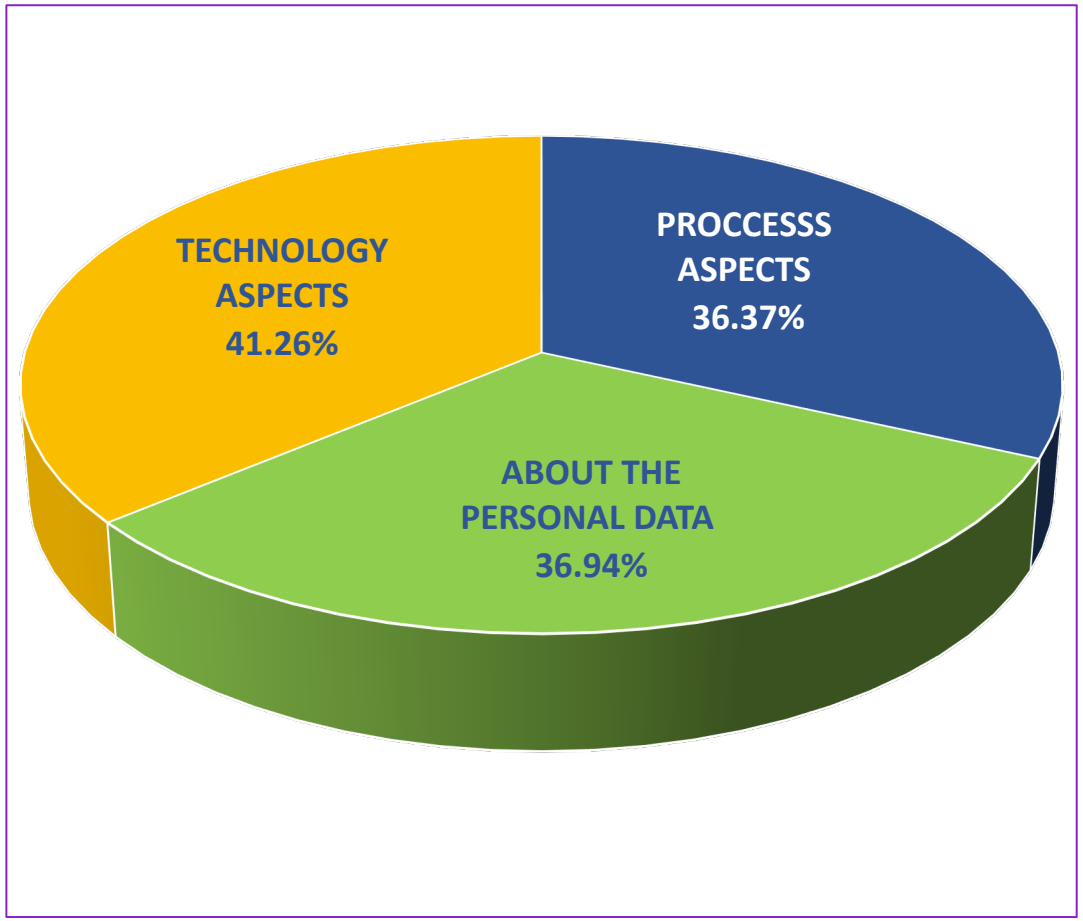
- LGPD - contract between the parties is required.
- GDPR – there is no requirement

Sanctions

- 4% annual revenue or 20 million Euros (the highest)
- 2% annual revenue with a limit of R $ 50 million

BRAZIL - ref. August 2020
Organisations of all size & sectors around the country

Average Compliance with Data Protection Law - LGPD – 40.05%



Risk Data

30.1% - had data violation incidents since the approval of the law (2018)

75.2% - of the organizations deals with personal sensible data

Source: Brazilian Software Association and Ernst & Young Global Limited

QUESTIONS ??

THANK YOU !!!

- **our site :**
  www.dnswomen.org
- **our twitter :**
  @dns_women
- **our facebook :**
  https://www.facebook.com/dnswomen
- **Email us :**
  vanda@scartezini.org