GLOBAL PRIVACY LAW DEVELOPMENTS
Vera Powell, Senior Corporate Counsel – Corporate Compliance and Privacy

Agenda

I. COVID-19 AND PRIVACY
II. RECENT PRIVACY AND DATA PROTECTION LAWS
   1. Post-GDPR Laws
   2. Brazil
   3. Nigeria
III. EMERGING TECHNOLOGIES AND PRIVACY
I. COVID-19 AND PRIVACY

Has your organization implemented new measures to combat the spread of COVID-19?

- Yes
- No
- I don’t know
Temperature Screening

- Employers may mandate temperature screening in the U.S.
- A regional German data protection office launched a probe into Apple’s plan to take the temperature of its store customers.
- Recent European Data Protection Board guidance refers to the requirements of national data protection and employment laws.

Temperature Screening

- **France:** Employers may not mandate temperature checks.
- **Netherlands:** Employers may conduct temperature screening, but processing of health data as a result of the screening is not allowed.
- **Germany:** Employers may mandate temperature checks, without recording the result of the screening.
- **Italy:** Employers may record the fact that the temperature is exceeded, but not the temperature reading.
Contact Tracing

• Most contact tracing apps use Bluetooth technology.
• The key question is: How is the data used and stored?
• The Google-Apple system localizes the data on the individual’s phone.
• EU Commission’s Guidelines minimize the intrusiveness of the app functionalities, including voluntary installation, deactivation of the app once the emergency is over, and data minimization.

Contact Tracing

• Singapore’s app uses Bluetooth signals between cellphones.
• Hong Kong requires smart wristbands for quarantine compliance.
• France’s contact tracing app uses Bluetooth technology.
• The UK has opted for a centralized app to store information about users’ contacts. The data is expected to be anonymized.
• The data collected by Italy’s voluntary app must be deleted no later than 12/31/2020.
Contact Tracing

As of mid-May:

- 47 contact tracing apps are used in 28 countries.
- 23% of the apps have no privacy policy; 53% don’t disclose how long they plan to store user data; and 60% have no publicly stated anonymity measures.
- Other digital tracking devices are used in 35 countries.

**Surveillance Technology**

- The government in South Korea uses smart phone location data, credit card data, and CCTV video.
- According to a [NY Times report](https://www.nytimes.com), in Israel, the government authorized a government agency to track millions of citizens’ cellphones during the pandemic.
- The government in Bulgaria adopted new powers to monitor people who have been placed in quarantine.

---

**Use of Drones**

- France recently banned the use of surveillance drones by police to monitor compliance with COVID-19 restrictions.
- Spain and Belgium have used drones to monitor the public’s compliance with lockdown rules.
- German police tested the use of drones in Dortmund and Dusseldorf.
What measures has your organization adopted to combat the spread of COVID-19?

- Sanitizing and/or social distancing
- Temperature screening
- Contact tracing
- Two or more of the above
- None of the above

Recap – Privacy Considerations

- Define the scope of COVID-19 data and legal bases
- Update your privacy notices
- Be proportionate and adhere to data minimization
- Retain information no longer than necessary
- Have security at the forefront of your mind
- Check national data protection and employment laws
- Conduct a Data Protection Impact Assessment
II. SELECT INTERNATIONAL PRIVACY LAWS

GDPR – The Modern Genesis

- **GDPR**: Introduced April 2016
  - Amended Feb. 2017 and March 2020
  - Effective Feb. 2018
  - Initially expected August 2020
- **China**: Passed in 2017/2018
  - Published May 27, 2019
  - Effective Jan. 2019
- **Thailand**: Published Aug. 27, 2019
- **California**: Amended Feb. 2017 and March 2020
  - Effective Jan. 2020
- **Japan**:
- **Australia**:
- **Nigeria**:
- **Brazil**:
Do any of these laws apply to your organization?

- All of them apply to my organization
- Some of them apply to my organization
- Few of them apply to my organization
- None of them apply to my organization

POLL

The Brazilian General Data Protection Law (LGPD) was published in August 2018.
- The LGPD defines personal data as any information related to an identified or identifiable natural person.
- Anonymized data is not considered personal data.
- The LGPD established the National Data Protection Authority ("ANDP").
• The LGPD lawful bases are largely aligned with the GDPR. They include:
  ✓ Consent
  ✓ Compliance with a legal or regulatory obligation
  ✓ Execution of public policies
  ✓ Contract or in a judicial or administrative procedure
  ✓ To protect life or physical safety
  ✓ To protect health or prevent fraud

• Prior consent is needed to transfer personal data to other jurisdictions unless certain conditions are met.
  The LGPD does not specifically address electronic marketing.
• Obtaining opt-in consent from consumers prior to sending marketing e-mails is recommended.
• Breach notification requirements if the breach is likely to result in risk or harm to data subjects.
• The LGPD provides for significant penalties.
  • Up to 2% of the revenues for a total maximum of R$50 million per infraction.
  • The enforcement by the ANDP is uncertain.

Brazil

• The Nigerian Data Protection Regulation (NDPR) was issued in January 2019 by the National Information Technology Development Agency (NITDA).
• NDPR protects the data of individuals residing in and outside Nigeria, as well as those of “Nigerian descent.”
• NDPR requires the appointment of a Data Protection Officer for Nigeria.

Nigeria
• The NDPR requires independent audits by Data Protection Compliance Officers (DPCOs).
• The DPCO must conduct an initial audit of a company’s data protection practices and file it with NITDA.
• After the initial audit, the DPCO must perform annual audits.

Lawful bases for processing:
- Consent
- Performance of a contract
- Compliance with a legal obligation
- Protect the vital interest of the data subject or another person
- Necessary to perform a task carried out in the public interest or as an official public mandate
- No “legitimate business interest”
• Processing by a third party should be memorialized through an agreement.
• A data protection clause is required.
• Personal data may be stored on servers outside Nigeria only if adequate level of protection is provided. Otherwise consent is required.
• Consent can be revoked or withdrawn.

NDPR requires the inclusion of certain information in a privacy policy.
✓ What constitutes the data subject’s consent
✓ Description of collectable personal information
✓ Purpose of the collection
✓ Technical measures used to collect and store personal information, such as cookies, web tokens, etc.
✓ Access of any third parties to personal data and the purpose of the access
• The penalties under the NDPR amount to 2% of the annual gross revenue or the sum of 10 million Naira (US$25,759.46), whichever is greater.
• Compliance with NDPR was extended from July 25, 2019 to October 2019.
• DPCOs can request an extension for compliance.
Which of the following characteristics are considered biometrics?

- Fingerprints
- Typing cadence
- Gait analysis
- All of the above
- None of the above

Biometrics

Physical
- Fingerprint
- Hand geometry
- Heartbeat monitoring
- Olfactory

Behavioral
- Voice pattern
- Typing cadence/finger movements on touch displays or trackpads
- Gait analysis

DNA
- Retinal/iris scan
- Ear shape (or lack thereof)
- Vein mapping

Image: Courtesy of King & Spalding LLP
Biometrics

- Law enforcement
- Access control and Single Sign On (SSO)
- Banking – transaction authentication
- Airport security
- Time and attendance
Biometrics

- Biometric data is likely sensitive information under comprehensive privacy laws.
- GDPR restricts its processing, subject to certain conditions (e.g., explicit consent).
- Potential further limitations may apply under Member State laws.

Global Regulation

Artificial Intelligence

- The process of intelligence being learned, developed, and used by machines.
- Collect vast amounts of individuals’ data
- Identify, re-identify, and track individuals
- Make inferences, predictions, and decisions about individuals
• OECD Principles on Artificial Intelligence:
  ✓ Inclusive growth, sustainable development, well-being
  ✓ Human-centered values and fairness
  ✓ Transparency and explainability
  ✓ Robustness, security, and safety
  ✓ Accountability

https://www.oecd.org/going-digital/ai/principles/

• GDPR requires individuals to be informed of the existence and consequences of profiling defined as
  “any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person . . .”

Cookies

- ePrivacy Directive requires consent to use cookies on websites.
- GDPR requires opt-in consent.
- European Court of Justice has found that pre-ticked checkboxes are insufficient.
• France fined Google $58 million for targeted advertising practices under the GDPR.
• Bavarian & Dutch regulators conducted “cookie sweeps” for website compliance.
• Spain fined IKEA under national law.