Dentsply Sirona

How to Build a Global Data Protection Plan

SCCE Berlin 11 March 2019

CONTENT

1. Dentsply Sirona and Data Privacy
2. Challenges and lessons learned from the GDPR implementation
3. Building a global data protection plan
Dentsply Sirona – The world’s largest provider of professional dental products

Dentsply Sirona:
- 16,000 employees
- Organizations in over 40 countries
- Our products are represented in 120 countries via global distributors

Product areas

<table>
<thead>
<tr>
<th>Consumables and Healthcare</th>
<th>Technology and Specialties</th>
</tr>
</thead>
<tbody>
<tr>
<td>Preventive</td>
<td>CAD/CAM</td>
</tr>
<tr>
<td>Restorative</td>
<td>Imaging</td>
</tr>
<tr>
<td>Prosthetics</td>
<td>Treatment Centers</td>
</tr>
<tr>
<td>Instruments</td>
<td></td>
</tr>
<tr>
<td>Endodontics</td>
<td></td>
</tr>
<tr>
<td>HealthCare (Wellspect)</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

The only manufacturer with comprehensive offering across all key categories for both general practitioners and specialists
Background on the GDPR project

- It expands the scope of the law to have extra-territorial effect in certain cases. GDPR impacts processes globally, not just within the EU, so it will affect all our Dentsply Sirona locations.
- Dentsply Sirona’s GDPR work was started during 2017 to ensure GDPR compliancy. Extensive work has been performed during 2017 and 2018 to understand GDPR, map all personal data and prepare for 25th of May.
- By liaising with external counsel a risk based approach was adopted to how to implement the GDPR program (based on available resources and activities that needed to be conducted). Focus was given on training on new policies and procedures, ensure existing high systems and processes were made compliant and putting in place contracts where necessary.
GDPR at Dentsply Sirona

Key focus areas in Dentsply Sirona’s GDPR program:

- **Organization**: DPO and DP Coordinators
- **Sensitive personal data**: Extra effort was put on securing compliance for sensitive personal data
- **Training and processes**: Educate and communicate with employees and support in incorporate GDPR in daily routines
- **Retention/deletion**: Delete data no longer needed or outside retention period
- **Policies and procedures**: Data protection manual, policies, SOPs

---

Key challenges from the GDPR implementation

- Challenging to get priority and engagement – mandatory but not so motivating
- Challenge to get resources – and the right resources
- Challenging to cope with the remaining historic inheritance and just-in-time-requests after May 25th
- One regulation, but in practice a lot of local laws deviations.
- Find a realistic level – risk approach
- Many new issues have been discovered during the project which have developed the overall program further.
- Extremely wide stretch – very cross functional in the organization, but also need access to experts
- Identify and capture all features of the different processing activities (not just separate parts of the processing)
- Align corporate and local processing activities
- Would have been easier in a perfect world where processes and information flows are documented and followed
- How to make this to continuous work – privacy by design, change management, audits etc.
Lessons learned from the GDPR implementation

- Communication is core – to all layers of the organization so people feel that they know what is happening and where we are in the project.
- Functional implementation and structuring is great in theory but not in practice – difficult to make business accountable.
- Get buy-in from and establish accountability with IT (central and local) from the start.
- Integrate local IT systems with corporate IT systems to minimize the processing means.
- Establish formal local organizational structures; to be data privacy’s eyes and ears.
- Provide easily accessible training and policy documentation.

CONTENT

1. Dentsply Sirona and Data Privacy
2. Challenges and lessons learned from the GDPR implementation
3. Building a global data protection plan
How was the project plan developed?

Define scope, existing compliance level and project team

Understand your personal data estate

Why

When

Who

Where

What
How was the project plan developed?

Define scope, existing compliance level and project team

Activities performed:

- Map out which active legal entities that are in scope and who the responsible people are for those entities (xx entities)
- Decide on contact persons going forward
- Number of employees
- The type of business
- Whether clinical trials are conducted
- Whether patient data is processed
- Reviewing existing policies and procedures

How was the project plan developed?

Define scope, existing compliance level and project team

Understand the legal framework and decide on approach

Activities performed:

- Map out which active legal entities that are in scope and who the responsible people are for those entities (xx entities)
- Decide on contact persons going forward
- Number of employees
- The type of business
- Whether clinical trials are conducted
- Whether patient data is processed
- Reviewing existing policies and procedures
How do the laws apply

- Think about history
- Remember colonization and conquest
- Commonwealth countries adopt a UK approach, so Singapore, South Africa, Canada, India and Australia have English style laws
- Spain and Portugal influence Argentina, Uruguay, Brazil and Macau
- France influences North Africa, Vietnam and Canada
How do the laws apply cont.

- USA – Sectorial laws
- Federal Laws:
  - The Financial Services Modernization Act (Gramm-Leach-Bliley Act (GLB))
  - The Health Insurance Portability and Accountability Act (HIPAA)
  - The HIPAA Omnibus Rule also revised the Security Breach Notification Rule
  - The Fair Credit Reporting Act The Controlling the Assault of Non-Solicited Pornography and Marketing Act (CAN-SPAM Act)
- State laws:
  - California Consumer Privacy Act of 2018 (effective from 1 January 2020).
  - Breach notification laws

Other countries with their own Data Protection laws

- Russia
- South Korea
- Malaysia
- Taiwan
- Indonesia
- Ukraine
- Israel
- Japan
- Hong Kong
- China
- Mexico
- Thailand
- United Arab Emirates
- Switzerland
- Turkey
- Philippines
- Peru
### Differences and similarities in global laws (selection)

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Australia</td>
<td>No</td>
<td>N/A</td>
<td>Mandatory in certain circumstances</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>€ 2 633 575</td>
<td>Yes</td>
</tr>
<tr>
<td>Brazil</td>
<td>No</td>
<td>Under LGPD</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>€ 11 746 482</td>
<td>Yes</td>
</tr>
<tr>
<td>Canada</td>
<td>No, Yes</td>
<td>Yes</td>
<td>Not yet in force at national level. Some state level requirements</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes. Not a legally defined term, but sensitive data requires consent.</td>
<td>Yes</td>
<td>€ 66 602</td>
<td>No</td>
</tr>
<tr>
<td>China</td>
<td>No, No</td>
<td>No</td>
<td>For &quot;network operators&quot; Yes?</td>
<td>Requires consent</td>
<td>Yes</td>
<td>Yes. In the cybersecurity law. No.</td>
<td>No</td>
<td>€ 128 963</td>
<td>No</td>
</tr>
<tr>
<td>Russia</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>Yes.</td>
<td>Yes</td>
<td>€ 10 000</td>
<td>No</td>
</tr>
<tr>
<td>Turkey</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>€ 165 849</td>
<td>Yes</td>
</tr>
</tbody>
</table>

### Deciding on approach - Creating one global program – is it possible?

- **Separate program for each country?**
- **One program fits all?**

Use existing GDPR program as a basis, adopt where necessary and carve out regions that are too specific to fit into the GDPR structure.
Dentsply Sirona’s approach

EEA (GDPR)  
Countries with EU influenced GDPR style laws (GDPR with some adoptions)

Law & Regulation

USA (US specific program)  
Rest of the world (small portions of GDPR program and some adoptions)

Australia  
Brazil  
Israel  
Japan  
South Korea  
Switzerland  
Turkey

China  
India  
Indonesia  
Thailand  
UAE  
Vietnam  
Russia

How was the project plan developed?

Define scope, existing compliance level and project team  
Understand the legal framework and decide on approach

Activities performed:
- Map out which active legal entities that are in scope and who the responsible people are for those entities (xx entities)
- Decide on contact persons going forward
- Number of employees
- The type of business
- Whether clinical trials are conducted
- Whether patient data is processed
- Reviewing existing policies and procedures
- Map out high level differences and similarities in global laws
- Decide the approach on how to structure the program – standardization vs. local market requirements.
- Categorize the countries into the set program approach
How was the project plan developed?

Define scope, existing compliance level and project team

Understand the legal framework and decide on approach

Consult with local legal advisors

Activities performed:

- Map out which active legal entities that are in scope and who the responsible people are for those entities (xx entities)
- Decide on contact persons going forward
- Number of employees
- The type of business
- Whether clinical trials are conducted
- Whether patient data is processed
- Reviewing existing policies and procedures

- Map out high level differences and similarities in global laws
- Decide the approach on how to structure the program
- Categorize the countries into the set program approach

Requested information from GDPR influenced countries

Data Protection Code  Employee Policy  Recruitment Policy  Website Notice  Cookie Statement

Consent language  LIA  International Data Transfers  DPIA  DPO

Sensitive data  Third party management  PbD  IS Policy  Acceptable Use

Social Media  Individual Rights  Data Disclosure  Data Destruction  Data Retention

Data Incidents
Requested information from ROW countries

Are there any local Data Privacy requirements?

Requested information from USA

What are the elements of a US privacy program and what would it cost to get assistance on creating policies/procedures for such program?
How was the project plan developed?

Define scope, existing compliance level and project team

Understand the legal framework and decide on approach

Consult with local legal advisors

Analysis of input from local law firms and the DS company

Activities performed:

- Map out which active legal entities that are in scope and who the responsible people are for those entities (xx entities)
- Decide on contact persons going forward
- Number of employees
- The type of business
- Whether clinical trials are conducted
- Whether patient data is processed
- Reviewing existing policies and procedures

- Map out high level differences and similarities in global laws
- Decide the approach on how to structure the program
- Categorize the countries into the set program approach

- Prepare working instructions to local counsel based on the set program approach
Action plan in GDPR influenced countries

Argentina, Australia, Brazil, Hong Kong, Israel, Japan, South Korea, Malaysia, South Africa, Switzerland, Turkey

Asked to implement

Data Protection Code, Employee Policy, Recruitment Policy, Website Notice, Cookie Statement, Consent language, LIA, International Data Transfers, DPIA, DPO, Sensitive data, Third party management, PbD, IS Policy, Acceptable Use, Social Media, Individual Rights, Data Disclosure, Data Destruction, Data Retention, Data Incidents, Mandatory Country specific requirements

Action plan in the ROW countries?

China, India, Indonesia, Mexico, Peru, Thailand, UAE, Vietnam, Russia, Taiwan

Asked to implement

Data Protection Code, Employee Policy, Recruitment Policy, Website Notice, Cookie Statement, Consent language, LIA, International Data Transfers, DPIA, DPO, Sensitive data, Third party management, PbD, IS Policy, Acceptable Use, Social Media, Individual Rights, Data Disclosure, Data Destruction, Data Retention, Data Incidents, Mandatory Country specific requirements
Action plan for the USA

How was the project plan developed?

Define scope, existing compliance level and project team
Understand the legal framework and decide on approach
Consult with local legal advisors
Analysis of input from local law firms and the DS company

Activities performed:
- Map out which active legal entities that are in scope and who the responsible people are for those entities (xx entities)
- Decide on contact persons going forward
- Number of employees
- The type of business
- Whether clinical trials are conducted
- Whether patient data is processed
- Reviewing existing policies and procedures
- Map out high level differences and similarities in global laws
- Decide the approach on how to structure the program
- Categorize the countries into the set program approach
- Prepare working instructions to local counsel based on the set program approach
- Focus countries based on risk (legal and business)
- Focus elements of the program based on risk in each focus country
- Budget for each country and element
Questions & Answers

Any questions?

Contact details

**Augusta Speiser**
Ethics & Compliance Director
Global Data Protection Officer
Dentsply Sirona
Augusta.Speiser@dentsplysirona.com
Thank you for your attention!