GDPR: What are the implications for you if you hold data in Europe?

Kim Gerhardt, Director

Edgar, Dunn & Company 40
Management Consultants Years Since 1978
What this session will cover

- What is GDPR? A brief discussion to set context...
- What are the implications to the travel sector?
- What do you need to do to be compliant?
Breaches of personal data have garnered significant attention.

**Equifax**: 145.5 million of its US customers might have been affected, which includes information such as Social Security numbers, birth dates and addresses.

**Hyatt**: Unauthorized access to payment card information from cards manually entered or swiped at the front desk of certain Hyatt-managed locations between March 18, 2017 and July 2, 2017.

**Facebook**: 87 million users affected by data breach where details of their accounts were shared with Cambridge Analytica.

**Orbitz**: Hackers may have accessed personal data 880,000+ accounts between October 2017 and December 2017.
The General Data Protection Regulation (GDPR) modernizes data protection for the digital age

- The GDPR is the biggest overhaul of data protection laws in 20 years
- GDPR’s aim is to enable people to have better control of their data
- One key element of the GDPR is that all personal data is owned by the data subject and not the organizations that collect it
- GDPR applies to all companies (anywhere in the world) that deal with personal data of EU data subjects
- Immediately applicable and enforceable by law
  - As good practice, Member States issue national legislation that defines the competent national authorities, inspection and sanctions on the subject matter
- The GDPR will apply starting May 25, 2018
What is Personal Data?

The GDPR applies to 'personal data' meaning any information relating to an identifiable person who can be directly or indirectly identified in particular by reference to an identifier.
GDPR equips data subjects with considerable rights to enable control of their data

- The right to be informed
- The right of access
- The right to rectification
- The right to erasure
- The right to restrict processing
- The right to data portability
- The right to object
- Rights in relation to automated decision making and profiling
Data controllers and data processors both fall under the regulation and are both accountable for data protection.

**Data Controller**
Entities that need to process personal data in order to do business; they determine the purposes and means of the processing of personal data.

**Data Processor**
Entities that take and/or process personal data on behalf of the Controller.

- Both are liable for the security of personal data.
- Both must maintain relevant documentation on processing activities.
- Both must implement measures that meet the principles of data protection.

Processing of personal data under the GDPR means carrying out any operation on personal data including:
- Collecting
- Recording
- Retrieving
- Using
- Organizing
- Disclosing
- Storing
- Deleting

4th Co-Brand Americas, 21st – 23rd May 2018
There are other requirements

🚀 Reporting data breaches
- The GDPR requires data controllers to notify the supervisory authority of a personal data breach within 72 hours of learning about the breach
- A data processor is required to notify a controller of a data breach “without undue delay”
- When a data breach occurs, controllers must notify individuals “when the personal data breach is likely to result in a high risk to the rights and freedoms of individuals” and they must do so “without undue delay”

💡 Data Protection Officers (DPO)
- Responsible for compliance with data protection laws and regulations
- Resides in the EU
- Mandatory for companies that process high volumes of personal data

🔒 Privacy by design: Products, systems, and processes must consider privacy during development
Under GDPR penalties can be imposed for non-compliance and negligence

➤ **Non-compliance** (violating the obligations of the processor and the controller) will result with in fines of up to **€10 million, or 2% of annual worldwide revenue**, whichever is higher

➤ **Negligence** (in case of breach including conditions of consent and infringement of data subject rights) goes even higher – up to **€20 million, or 4% of annual worldwide revenue**, whichever is higher

**Much is Unknown at this point…**

➤ What types of organizations will the governing bodies go after?

➤ How aggressive will they be?

➤ On which aspects of the GDPR will they focus?

➤ How will they test compliance?
What is the impact of GDPR?

➤ Companies need to **adapt their business processes** to comply with the GDPR
  ▪ Shift from opt-out to opt-in rules
  ▪ Communicate their intention with the data and who is responsible for storing and processing it
  ▪ Create mechanisms for customers to access to their data or enable portability
  ▪ Create mechanisms to identify a personal data breach and report it within 72 hours

➤ Data controllers need to **execute contracts** with data processors and **conduct due diligence** to ensure data processors are GDPR compliant

4th Co-Brand Americas, 21st – 23rd May 2018
The travel sector has unique challenges

- Transportation companies collect significant personal customer data to tailor propositions and create competitive advantage
  - Marketing new promotions, products, services
  - Streamlining process by sharing with suppliers
  - Improving the customer experience

- IT infrastructure of an airline is complex
  - Customer information can reside in different systems and multiple databases, such as the app, website, billing, servicing, marketing, and booking systems
  - Multiple legacy systems collected over time and through M&A activity

Processes, systems, and data management will need to reviewed brought in line with the new regulations

4th Co-Brand Americas, 21st – 23rd May 2018
Data controllers and data processors established in the EU that process personal data in the context of the activities of the EU establishment, regardless of where the processing takes place.

Data controllers and data processors not established in the EU that process EU data subjects' personal data in connection with offering goods or services or monitoring their behavior.

“Establishment implies the effective and real exercise of activity through stable arrangements”
GDPR to become global standard?

“[Air Canada’s policy is to follow data laws that] comply with as many other applicable laws as possible, or at least those that pose the greatest risk if you don’t comply.”

Rachelle Henderson, Senior Counsel for Labor, Air Canada

“The best approach is to identify the highest standards and apply them across the board. [Air New Zealand] has internalized privacy principles and adopted a privacy by design culture.”

Karen Clayton, General Counsel, Air New Zealand

“...GDPR is a gamechanger. [...] As onerous as it is and as stringent as it is, it’s tangible, it’s clear, and I think it’s going to become the global default.”

Jeffrey Poston, Partner, Crowell & Moring
What do you need to do to become compliant?

- Obtain explicit **consent** for each data use case; Develop customer opt-in process that is clear and recordable
- Develop and provide a **clear privacy notice** including what data, why it is collected, how it will be used, who it will be shared with, how long it will be kept, and data subject rights.
- Provide **data portability** and be able to export data in a common format
- Establish policies and procedures to detect, report, and investigate a **personal data breach**

- **Conduct data discovery and mapping**
  - Identify all personal information and understand where it flows and where it is stored
  - Document this understanding in the form of network diagrams, data flow diagrams, and process descriptions.
  - Audit personal data and its purposes, and be prepared to present data, explain the purpose of collection, and delete unnecessary data

4th Co-Brand Americas, 21st – 23rd May 2018
What do you need to do to become compliant?

- Review contracts about personal data exchange with partners
  - Codeshare partners, travel agencies, catering suppliers, passenger assistance service companies, cloud storage providers...
  - Contracts should include an explanation of how they meet the obligations for data protection, including their plan to: secure data, keep it up-to-date, and explain to individuals where and how they have obtained the data

- Conduct and document data protection impact assessments to assess risk, using information gathered from the data mapping exercise as well as information about the systems and networks used to process this data

- Develop process to respond to Data Subject Access Requests

- Appoint a Data Protection Officer located in the EU with responsibility over data protection compliance
Questions
Appendix: About Edgar, Dunn & Company
Edgar, Dunn & Company (EDC) is an independent global financial services and payments strategy consultancy

**EDC: Independent, Global, Financial Services**

- Founded in 1978, the firm is widely regarded as a trusted advisor to its clients, providing a full range of strategy consulting services, expertise and market insight, and M&A support.

- EDC has been providing thought leadership to its client base working with:
  - More than 40 European banks & card issuers/acquirers
  - Most of the top 25 US banks and credit card issuers
  - Many of the world's most influential mobile payments providers
  - All major international card associations / schemes & many domestic card schemes
  - Many of the world's leading merchants, including major airlines

**EDC Office Locations**

- London
- Frankfurt
- Paris
- San Francisco
- Istanbul
- Sydney

**EDC Key Metrics**

- Financial services and payments focus
- Five office locations worldwide
- Independent - owned and controlled by EDC Directors

- +1,000 projects completed
- +250 clients in 40 countries & 6 continents

4th Co-Brand Americas, 21st – 23rd May 2018
For 40 years Edgar, Dunn & Company has served the world’s leading companies in their field

Payment Networks
Global payment networks, domestic debit schemes

Merchant Acquirers, Processors & Payment Gateways
Acquirers, processors, value-added resellers, J.P. Morgan

Banks & Financial Institutions
Payment cards: credit, debit, prepaid, commercial, virtual/one-time; ACH

Payment Vendors & Solution Providers
POS manufacturers and distributors, card manufacturers, service providers

Regulators, Wholesale Pricing & Payment Economics
Legislative development/responses/inquiries, new product pricing, costing studies

Alternative Financial Services & The Underserved
Money transfer, remittances, check cashing, kiosk agents, cash mgmt.

Online Innovators
Mobile, eWallets, Tokenization, EMV, Blockchain, X-border remittances

Transaction Advisory Services
M&A, due diligence, acquisition identification, valuations, strategic assessments

Travel, Transit & Transportation
GDS, airlines, rail networks, hotels, product and service providers

Payment Networks
Global payment networks, domestic debit schemes

Merchant Acquirers, Processors & Payment Gateways
Acquirers, processors, value-added resellers, J.P. Morgan

Banks & Financial Institutions
Payment cards: credit, debit, prepaid, commercial, virtual/one-time; ACH

Payment Vendors & Solution Providers
POS manufacturers and distributors, card manufacturers, service providers

Regulators, Wholesale Pricing & Payment Economics
Legislative development/responses/inquiries, new product pricing, costing studies

Alternative Financial Services & The Underserved
Money transfer, remittances, check cashing, kiosk agents, cash mgmt.

Online Innovators
Mobile, eWallets, Tokenization, EMV, Blockchain, X-border remittances

Transaction Advisory Services
M&A, due diligence, acquisition identification, valuations, strategic assessments

4th Co-Brand Americas, 21st – 23rd May 2018
EDC’s Advisory Services covers multiple functional areas

- **Strategy Development**
  - Enterprise & Market entry strategies
  - Credit and debit card strategies
  - Merchant / acquirer strategies
  - Retail/wholesale strategies
  - B2B payment strategies

- **Risk Management**
  - Risk management strategies
  - Credit and fraud risk strategies
  - Fraud prevention and detection
  - Authentication strategies
  - Benchmarking and best practices

- **Profitability and Pricing**
  - Customer segmentation analysis
  - Portfolio profitability
  - Payment Network pricing
  - Cost studies
  - Product pricing

- **Process Improvement**
  - Payment dispute solutions
  - Back-office process improvement
  - Third-party processor evaluation
  - Scheme & regulatory compliance
  - Payment roadmap development

- **New Product Development**
  - Market research
  - Market opportunity assessment
  - Product development
  - Debit, credit, and smartcards
  - Mobile/wireless payments
  - B2B payments integration

- **Transaction Advisory Services**
  - Buy-side support (target selection, bid strategy)
  - Due diligence
  - Valuation
  - Information Memorandums

4th Co-Brand Americas, 21st – 23rd May 2018
## Our approach is based on senior professional involvement and focuses on providing actionable advice

<table>
<thead>
<tr>
<th>Approach</th>
<th>Description</th>
<th>Benefits</th>
</tr>
</thead>
<tbody>
<tr>
<td>Our Most Senior Professionals Consult</td>
<td>- Our most experienced professionals on every project&lt;br&gt;- Directors are active participants in engagements&lt;br&gt;- Our professionals average more than 20 years experience in both industry and consulting</td>
<td>Clients benefit from deep industry expertise and years of hands-on experience</td>
</tr>
<tr>
<td>We Deliver Global Services</td>
<td>- Full EDC firm expertise on every project&lt;br&gt;- Projects staffed with resources from multiple markets&lt;br&gt;- Unique ‘one-firm’ style of consulting</td>
<td>This approach helps our clients implement winning strategies globally</td>
</tr>
<tr>
<td>We Help Implement Our Advice</td>
<td>- Focus on initiatives most critical to our clients business&lt;br&gt;- Work side-by-side with clients to achieve desired goals&lt;br&gt;- Our focused project teams collaborate with clients to meet desired objectives</td>
<td>We conclude projects only after our clients are satisfied with the knowledge transferred</td>
</tr>
<tr>
<td>We Invest In Long-Term Relationships</td>
<td>- We view our clients as partners and we invest significant time and resources to understand their unique characteristics and issues&lt;br&gt;- Our goal is to maximize value of their investment in us</td>
<td>Our clients have trusted us to help them shape their strategies for over 30 years</td>
</tr>
</tbody>
</table>
We have proven approaches to assist clients in some of the most challenging areas of payments.
Conducted a review of current payments processing infrastructure for a global travel industry payment association, identified alternative approaches to the provision of a more efficient, functional and flexible infrastructure, developed an RFP for the same, and currently supporting the evaluation of the RFP.

Worked with a national passenger rail company to understand their current payment processing environment and recommend a new payment processing architectural structure for processing payments in a secure, fast, and cost effective manner. Additionally, we recommended a process for evaluating payment processing vendors (including acquirers) within the scope of the recommended architecture. Finally, we recommended additional alternative payment methods for the company to take under consideration in addition to offering credit cards as payment for travel.

Conducted a review of current payments processing infrastructure (terminal driving, internet payment gateway, transaction acquiring, stand-in authorization, switching, clearing, settlement, risk management and prepaid card issuer processing) for a global top 20 retailer, short-listed alternative approaches / solutions, prepared an RFP to top vendors, and currently supporting the evaluation of the RFP.

Assisted a public transport ticketing authority (covering rail, bus and ferry services) during the evaluation phase of the electronic ticketing system (ETS) tender process. EDC reviewed and advised on a specific section of the tenders that referred to options for the ETS migration to an account-based smartcard.

Advised a global airline payment program seeking to replace its current payment transaction switching, authorization, clearing and settlement system. Reviewed the current payments infrastructure; developed high level requirements; conducted industry research of available vendor options; assisted in the development and evaluation of the RFP to replace the infrastructure.

Supported an automotive financial services bank in the development of a business case and P&L model for a new cobranded credit card. Developed the financial models and frameworks to support analysis of the planned product, including forecasting product and line of business P&L’s, portfolio sizing and performance metrics, and trade-offs in portfolio NPV from various pricing strategies.
Select Engagements (continued)

- Conducted a full strategy development project for a European-based acquirer specialized in the travel sector. Project included full situation analysis, development of strategic options, and a detailed business case supporting the recommended strategy. Since then the strategy has been successfully implemented.

- Conducted a review for a major global alternative payment method of alternative payment gateway and acquiring arrangements, including discussions with vendors, payment networks, financial institution acquirers and payment gateways, so as to identify the most cost effective and low-risk payment processing options available.

- Assessed the financial benefits, implementation requirements, and potential issues related to alternative forms of payment for direct online sales for a major global airline in five countries.

- Supported a top 5 European airline in its contract negotiation with its major merchant acquirer (resulted in a significant improvement in contract terms in excess of a 10% cost reduction).

- For a provider of payment products focused on the travel segment, conducted a process improvement project that included mapping existing policies, business processes and tools with a view of identifying opportunities to automate and streamline current processes.

- Conducted several strategy workshops and developed a strategic business plan for a leading European online payment transaction processor and acquirer focusing on high-risk e-commerce merchants.

- Completed a global fraud trend and end-state project for an international payments network. This study included POS as well as online payments, and included all types of fraud including practices for authenticating customers to protect against the emerging fraud sources of identity theft, mass data compromise, phishing, pharming, and probing.

- Assessed the potential for a motorcycle brand to develop a private label credit card product for its customers and dealer relationships.