DORSEY™
always ahead

THE EU GENERAL DATA PROTECTION REGULATION: COMPLACENCY IS NO LONGER AN OPTION

Ron Moscona

DORSEY™
always ahead

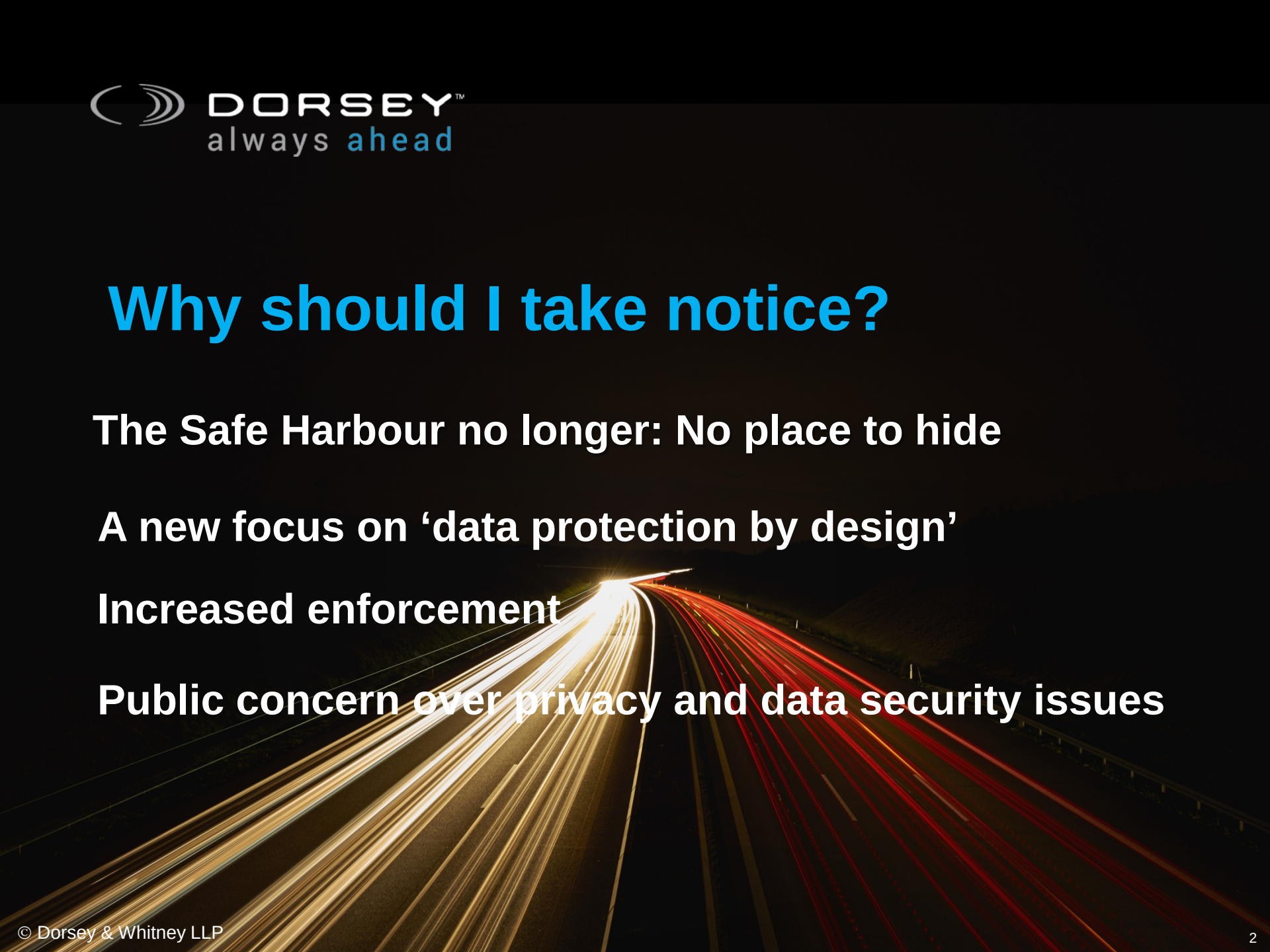
Why should I take notice?

The Safe Harbour no longer: No place to hide

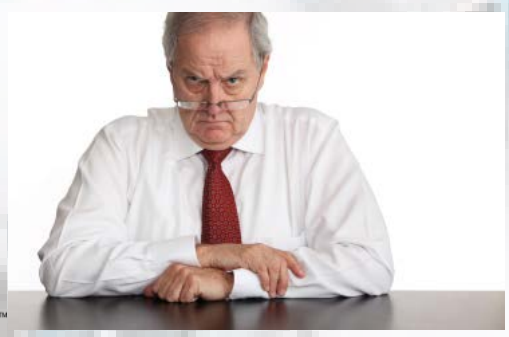
A new focus on ‘data protection by design’

Increased enforcement

Public concern over privacy and data security issues



Why is it important?



DORSEY always ahead

employees

customers

account holders

debtors

candidates

competitors

users/subscribers

patients

channels

Influencers/promoters

suppliers

clients' data

Name

Email

Address

Telephone number

Post code

Age/gender

Employment/profession

Purchasing records

Browsing history

Affiliations/memberships

IP address/MAC number

Credit history

Health information

Preferences/profiling

Risk profile

Images/posts

correspondence

EU casts a wider net

- Customers
- Subscribers
- Users
- Readers
- Online services
- Profiling
- Personalising
- Targeting

Territorial reach

(I) Processing is in the context of an establishment: -

- of a controller in a Member State; or
- of a processor in a Member State

(II) Processing of personal data of data subjects in the EU by a controller/processor not established in the EU, relating to: -

- Offering of goods or services (paid or free) to EU data subjects, or
- Monitoring of EU data subjects' behavior

A new regulatory framework

- One ring to rule them all – uniform rules for all EU member states (with limited room for national variations)
- Data protection by design – a proactive approach to compliance
- Ratcheting up enforcement – strengthened tools for regulators
- A powerful central EU-level regulatory body

Regulatory enforcement powers

- Audit and investigate
- Access all personal data of controller/processor
- Access premises/computer systems of controller/processor
- Issue compliance orders
- Order temporary/permanent ban on processing
- Order rectification/erasure
- Order temporary/permanent cessation of data flows outside the EU
- Withdraw/order the withdrawal of compliance certifications
- Impose administrative penalties up to 4% of annual turnover or EUR20m

Compliance fundamentals

Is it legal to collect/keep the data? What data should I keep?

Is data subjects consent required?

Is it enough to post a privacy policy on my website?

Do I need to engage with regulatory authorities?

Who gets access to the data? Can I keep on an open system?

Can I keep the data outside of the EU? Can I transfer it to the U.S.?

How do I maintain the data? Can I keep it on the cloud?

Regulatory burdens

- ✓ Appointment of compliance officer
- ✓ Preparation of impact assessment
- ✓ Engagement with regulator
- ✓ Reporting data breaches
- ✓ Records keeping
- ✓ Certification/codes of conduct
- ✓ Data protection by design

Data collection – opt-in/opt-out

Data collection - approvals

Access control

Encryption/data security

Anonymisation/pseudonymisation

Repurposing – notification to data subjects/consent

Data cleansing protocols

Data portability

Data tracking (3rd party notifications)

Duties to data subjects

- Processing notification
- Consent (opt-in/opt-out)
- Responding to data subject requests
- Rectification/updating
- Right to be forgotten (erasure)
- Notification of rectification, erasure or restriction to 3rd parties
- Right of data portability
- Right to object - profiling, direct marketing, automatic decision making, harmful processing

Legal documentation

- Consent forms
- Data processors contracts
- Joint controller contracts
- Information to be given to data subjects
- Privacy policy
- Data processing impact assessment

Rules relating to consent

- Free, specific, informed and unambiguous
- By statement or affirmative action
- Consent may be withdrawn
- Consent folded into Ts&Cs
- Consent as part of privacy policy
- Data contributed/posted by data subject
- Obtaining consent for processing of sensitive data
- Obtaining consent from children

Exporting data outside the EU

- ✓ **Privacy Shield/certifications**
- ✓ **Model Contractual Clauses**
- ✓ **Binding Corporate Rules**
- ✓ **Data subject consent**

- ➢ **Notification requirement**

Sensitive data – a stricter regime

Data relating to:

- racial/ethnic origin
- political opinion
- religious/philosophical beliefs
- trade union membership
- genetic data
- biometric (ID) data
- health
- sex life or sexual orientation
- criminal convictions and offences

- A higher threshold for ‘legal basis’
- A higher regulatory compliance burden
- Specific rules in relation to patients’ medical records

What amounts to ‘high risk’?

- Large databases
- Profiling data
- Automatic processing
- Health data
- Employment
- Confidential data (financial, legal, private)
- Big data
- Data not contributed by subjects
- Marketing data