ARE YOU GDPR-READY?

Preparing for the new law and ensuring a privacy-protective travel programme

KEY ELEMENTS OF THE GENERAL DATA PROTECTION REGULATION (GDPR)

Is your company ready?

Higher sanctions
Companies can be fined up to 4% of total global turnover for failure to comply.

Vendor responsibilities
New contractual terms required in data processing agreements. Vendor processors are directly regulated, and vendors attempting to avoid controller responsibility where it applies are breaking the law.

Data protection officers
Most companies are required to appoint someone responsible for independently overseeing compliance.

More individual rights
Traditional rights to access, correct and delete data now supplemented with right to be forgotten, right to data portability.

Governance
Companies are required to maintain demonstrable evidence of the lawfulness of their privacy and data protection programme.

Privacy by design
Products must undergo privacy impact assessments built into product development process. Defaults must be privacy protective.

Wider scope
Application to activities that originate outside the EU but impact EU residents' personal data.

Higher bar for consent
Consent must be specific, informed and revocable. Other justifications may be more appropriate for core services .

Harmonisation
One law applies across the EU – a regulation has direct effect. Member state DPAs will still vary in enforcement philosophy, though.

GLOBAL BUSINESS TRAVEL

DATA CONTROLLERS AND PROCESSORS

CONTROLLER

- Determines the "purposes and means" of processing
- Directly responsible for data protection compliance

PROCESSOR

- Processes data only at the direction of the controller
- No direct responsibility or liability for compliance

> Example No. 7: Travel agency (1)
>
> A travel agency sends personal data of its customers to the airlines and a chain of hotels, with a view to making reservations for a travel package. The airline and the hotel confirm the availability of the seats and rooms requested. The travel agency issues the travel documents and vouchers for its customers. In this case, the travel agency, the airline and the hotel will be three different data controllers, each subject to the data protection obligations relating to its own processing of personal data.

– Article 29 Opinion 1/2010

GLOBAL BUSINESS TRAVEL

PURPOSES AND MEANS – MAKING A DETERMINATION

Is your vendor a data controller?

1. Is this vendor required to make complex decisions about how, what and why information is processed?
2. Is this vendor transparent to end users?
3. Is this vendor in the best position to take care of regulatory formalities?

GLOBAL BUSINESS TRAVEL

INTERNATIONAL DATA TRANSFERS

recognising multiple lawful mechanisms

BINDING CORPORATE RULES

Custom set of internal, binding corporate policies and external commitments

- Approved by each individual Data Protection Authority in Europe and recognised by other authorities around the world
- Authorises transfer around the world
- Favoured in new GDPR

PRIVACY SHIELD

European Commission recognised self-certification process in the United States

- Doesn't require approval by each DPAs
- Self-certification process
- Authorises transfer to US only
- Currently on shaky ground

EU MODEL CLAUSES

Contractual template obligating vendor to comply with EU law

- Can't be negotiated or amended
- Not tailored to individual services

ADEQUACY

Keep it where the law will apply adequate protections

- In the EU or a country on an approved list (Canada, New Zealand, Uruguay, Argentina)
- Doesn't really work for travel – the data has to go where travellers do

GLOBAL BUSINESS TRAVEL

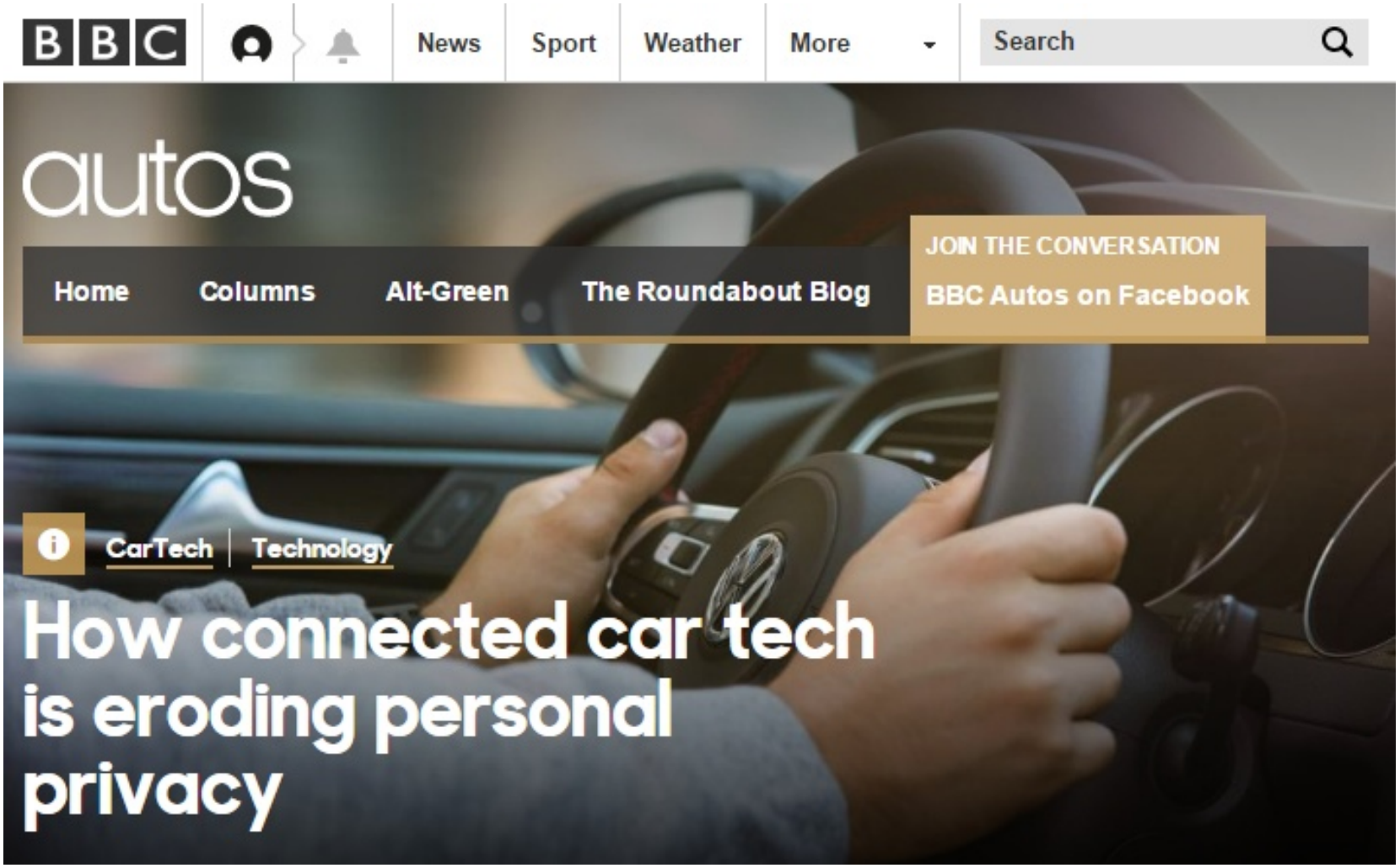
theguardian

home › tech | UK | world | politics | sport | football | opinion | culture | business | all

Samsung

Samsung's voice-recording smart TVs breach privacy law, campaigners claim

US consumer rights group Epic claims Samsung has breached the privacy of its users, and is demanding an FCC investigation



TECHNOLOGY

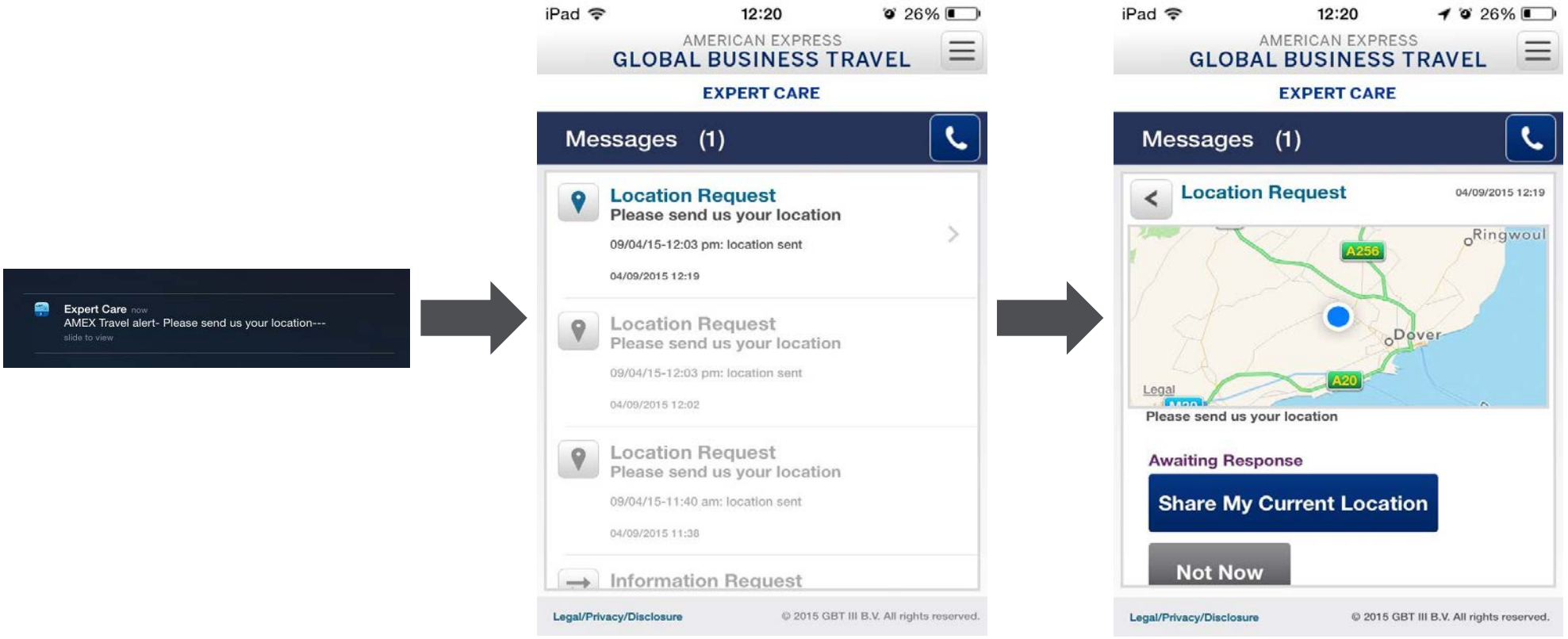
Apple faces privacy breach charges with its secret user tracking file

BY **MONAMI THAKUR** ON
04/21/11 AT 6:38 AM

4

PRIVACY BY DESIGN

usable design creates good privacy



PREPARING FOR THE GENERAL DATA PROTECTION REGULATION

Questions to ask your travel company

Personnel
Do you have a data protection officer or team responsible for data protection compliance?

Transparency
Do travellers see a privacy statement that accurately and completely describes your services and the role you play in providing them?

Consent
Do you rely on the right protocols for lawful processing? Are travellers asked for consent only where it can be specific, informed and revocable.

Privacy by design
Are privacy impact assessments a regular part of your product development process to ensure that your products meet privacy by design best practices?

Vendor risk
Do you take responsibility for appropriately assessing and managing vendors who will process traveller information?

Individual rights
Do you have protocols for assuring data subjects can access, correct or delete their data as the law requires?

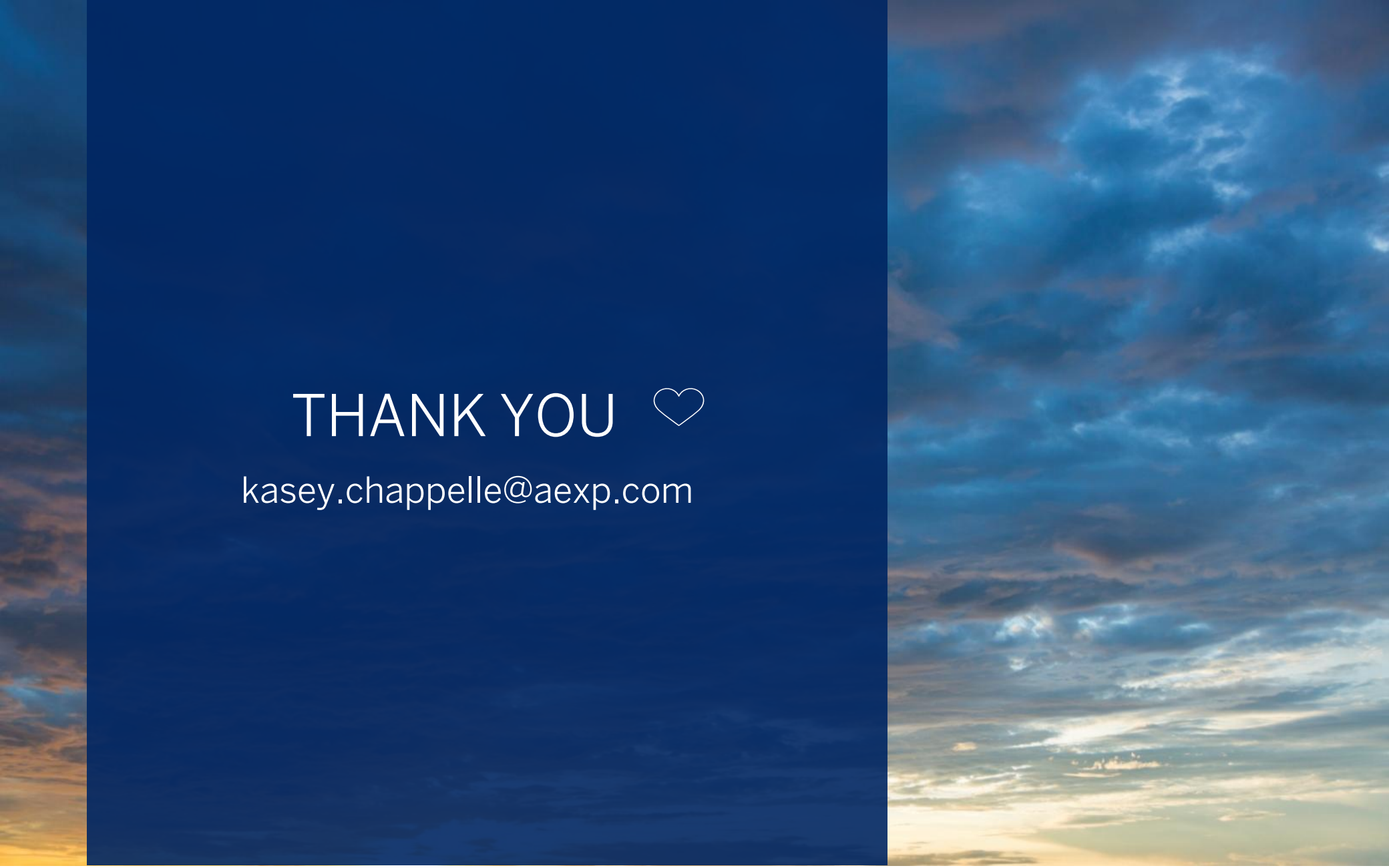
International transfers
Do you have a data transfer mechanism in place – like BCRs, Privacy Shield , model clauses or adequacy, that remains lawful under court decisions and the new law?

Breach
Do you maintain appropriate data breach and incident response protocols?

Accountability
Do you maintain demonstrable evidence of the lawfulness of your privacy and data protection programme?

Responsibility
Travel services frequently require independent judgment calls about how data is collected, used and shared. Are you willing to take responsibility as a data controller or data processor as required by law for your services?

GLOBAL BUSINESS TRAVEL



THANK YOU ♡

kasey.chappelle@aexp.com

GLOBAL BUSINESS TRAVEL