FLINN

GDPR ~ ISSUES IN M&A TRANSACTIONS

LEONARD HAWKES &
BENOIT SIMPELAERE

14TH INTERNATIONAL M&A CONFERENCE
1-3 NOVEMBER 2019 | VERSAILLES | FRANCE

AGENDA

THE POTENTIAL ISSUES ARE REAL

ANALYSIS

TOWARDS BEST PRACTICE

THE POTENTIAL ISSUES ARE REAL

Marriott
INTERNATIONAL

Marriott International Update on Starwood Reservation Database Security Incident

BETHESDA, MD, July 9, 2019 – Marriott International announced that the UK Information Commissioner's Office (ICO) has communicated its intent to issue a fine in the amount of £99,200,396 against the company in relation to the Starwood guest reservation database incident that Marriott announced on November 30, 2018. Marriott has the right to respond before any final determination is made and a fine can be issued by the ICO. The company intends to respond and vigorously defend its position.

Marriott International's President and CEO, Arne Sorenson, said: "We are disappointed with this notice of intent from the ICO, which we will contest. Marriott has been cooperating with the ICO throughout its investigation into the incident, which involved a criminal attack against the Starwood guest reservation database.

"We deeply regret this incident happened. We take the privacy and security of guest information very seriously and continue to work hard to meet the standard of excellence that our guests expect from Marriott."

The Starwood guest reservation database that was attacked is no longer used for business operations.

For more information about the Starwood guest reservation database incident, please visit https://info.starwoodhotels.com/

About Marriott International

Marriott International, Inc. (NASDAQ: MAR) is based in Bethesda, Maryland, USA, and encompasses a portfolio of more than 7,000 properties under 30 leading brands spanning 131 countries and territories. Marriott operates and franchises hotels and licenses vacation ownership resorts all around the world. The company now offers one travel program, Marriott Bonvoy™, replacing Marriott Rewards®, The Ritz-Carlton Rewards®, and Starwood Preferred Guest®(SPG). For more information, please visit our website at www.marriott.com, and for the latest company news, visit www.marriottnewscenter.com. In addition, connect with us on Facebook and @MarriottIntl on Twitter and Instagram.

Source: Marriott International, Inc's filing with the US Securities and Exchange Commission

ICO Notice of Intention to Fine Marriott International £99,200,396

Information Commissioner Elizabeth Denham said:

- "The GDPR makes it clear that organisations must be accountable for the personal data they hold. This can include carrying out proper due diligence when making a corporate acquisition, and putting in place proper accountability measures to assess not only what personal data has been acquired, but also how it is protected".

Source: ICO 9 July 2019

Marriott International's President and CEO, Arne Sorenson, said:

- "We are disappointed with this notice of intent from the ICO, which we will contest. Marriott has been cooperating with the ICO throughout its investigation into the incident, which involved a criminal attack against the Starwood guest reservation database.
- "We deeply regret this incident happened". … "The Starwood guest reservation database that was attacked is no longer used for business operations".

Source: Marriott International 9 July 2019

FLINN

GDPR SUMMARY POINTS

- EU Regulation 2016/679, effective as from 25 May 2018
- Gives individuals ('data subjects') stronger control over and protection for their personal data.
- Data controllers and processors must comply with particular requirements on fair processing, organisation and security.

Geographic scope:

- Organisations who offer goods or services to data subjects present in the EEA (even if the organisation is not itself present here).
- Transfers of data to third countries

Penalties

- Up to €20million or 4% of annual global revenue, whichever is greater, for the most serious infractions
- Up to €10million or 2% of annual global revenue, whichever is greater, for infractions considered less serious

THE POTENTIAL ISSUES ARE REAL

Source: iapp.org

GDPR ONE YEAR ANNIVERSARY (25 May 2019)

- 280,000+ Cases received by DPAs
- 144,000+ Individual complaints
- 89,000+ Data Breach notifications

➢ €56 million+ of fines arising from enforcement actions

FLINN

1. California Consumer Privacy Act (CCPA)

1 January 2020

2. Brazil 'Lei Geral de Proteção de Dados' (LGPD)

1 August 2020

3. India Personal Data Protection Bill

4. New Zealand Privacy Bill

DATA PRIVACY RULES ARE BEING ADOPTED WORLDWIDE

Organisations must be accountable for the personal data they hold

"A variety of personal data contained in approximately 339 million guest records globally were exposed by the incident, of which around 30 million related to residents of countries in the European Economic Area (EEA). Seven million related to UK residents".

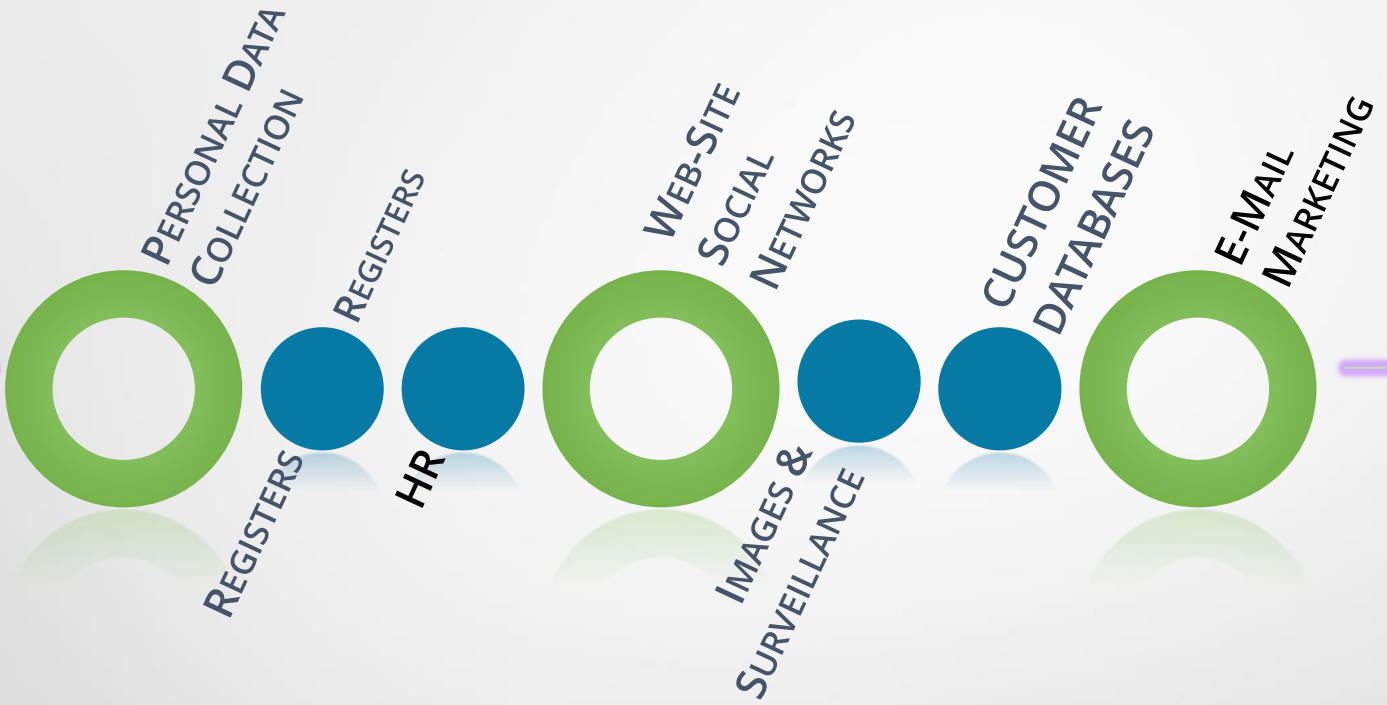
ICO Statement: Intention to fine Marriott International, Inc more than £99 million under GDPR for data breach

Organisations must be accountable for the personal data they hold

"It is believed the vulnerability began when the systems of the Starwood hotels group were compromised in 2014. Marriott subsequently acquired Starwood in 2016, but the exposure of customer information was not discovered until 2018".

ICO Statement: Intention to fine Marriott International, Inc more than £99 million under GDPR for data breach

EXTERNAL



INTERNAL

FLINN

IMPACT ON HEADS OF TERMS

ANALYSIS 1

- Is the business to be acquired B2B or B2C?
- Is there a website and does it at a minimum have a privacy policy and a cookies policy?
- Are there significant data-bases containing (customers) personal data?
- What is the value/importance to the buyer of such data-bases?
- Does the Seller have full rights to transfer the personal data?

IMPACT ON DUE DILIGENCE

ANALYSIS 2 / Part 1

- ❑ Is GDPR a separate heading of the DD request? (Or did you just include it as part of the ICT or Intellectual Property requests?

Some abbreviated examples of the sort of questions that you may wish to ask:

- ✓ Is Target a personal data 'controller' and / or 'processor' ? Why ?
- ✓ Do you have a GDPR compliance system – who is the provider – when was it introduced?
- ✓ Please provide a copy of the 'register' for processing of personal data if you have prepared one;
- ✓ Do you have a Data Protection Officer – if not who is the lead on GDPR compliance?
- ✓ What training have Targets employees who deal with personal data had on GDPR? How often is it updated?

IMPACT ON DUE DILIGENCE

ANALYSIS 2 / Part 2

- ❑ Concerning Target's website
- ✓ Details of the privacy policy - when was the privacy policy last up-dated?
- ✓ Details of the cookies policy - when was the cookies policy last up-dated?
- ✓ Details of the Terms and Conditions of Use

IMPACT ON DUE DILIGENCE

ANALYSIS 2 / Part 3

- ✓ Copies of all data processor contracts for data subjects outside your organisation.
- ✓ Copies of all data-processor contracts in respect of personal data of employees and consultants (HR, payroll, social security for example)
- ✓ Copies of all data subject requests (eg. requesting access to personal data) together with documents evidencing the data controller's response (including any correspondence Data protection Authority).
- ✓ If personal data is transferred outside the European Economic Area, details of the countries concerned and details of basis for such transfers: adequacy, standard contractual clauses or consent and if consents details of the consents given for cross-border data transfers.
- ✓ Details of any failure (or alleged failure) to comply with the requirements of the Data Protection laws since 25 May 2018.

IMPACT ON SELLERS REPS & WARRANTIES,

- What is the risk assessment?
- Is a warranty to the standard of the Seller's (best) knowledge satisfactory?
  - "To the Sellers' best knowledge, the (Group) Companies comply with and conduct their business in accordance with all applicable Laws relating to data protection. None of the (Group) Companies have received any written notification from any Governmental Authority regarding any actual or alleged violation of any such Laws by any (Group) Company. "

SPECIFIC INDEMNITY

- Or given the potential liabilities and the mandatory compliance obligations does the DD indicate the need for a specific indemnity for:
  - 'Any Loss incurred in relation to any judicial or administrative action, suit, claim, investigation, or proceeding against Target relating to any breach of the GDPR that occurred during the period from 25 May 2018 to [the Closing Date]'.

Towards best practice?

Do you also have experience that you would you like to share?

THANK YOU FOR YOUR KIND ATTENTION

Benoit Simpelaere

benoit.simpelaere@flinn.law

T. +32 (0)2 274 51 83

F. +32 (0)2 512 01 38

Leonard Hawkes

leonard.hawkes@flinn.law

T. +32 2 274 51 88

F. +32 2 274 51 81

FLINN

www.flinn.law

and … save the date for the FLINN Cup 2020! Saturday, 5th of September 2020

FLINN