SANS SUMMIT NEW YORK CITY AUGUST 19, 2018

Alexander Blumrosen

Attorney admitted in Paris, France and New York

KAB Avocats, Paris

DATA BREACH NOTIFICATIONS UNDER THE GDPR IN FRANCE

Agenda

- GDPR Data Breach requirements
- Breach Notifications in France
- Investigations in Civil Law countries; Blocking Statutes, privilege
- Assessment of compliance requirements and enforcement under GDPR

GDPR ARTICLE 33 – NOTIFICATION REQUIREMENT (33(1))

1. In the case of a personal data breach, the controller shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the supervisory authority competent in accordance with Article 55, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. …

GDPR ARTICLE 33 – CONTENTS OF NOTIFICATION (ART. 33(3))

The notification referred to in paragraph 1 shall at least:

- describe the nature of the personal data breach including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned;
- communicate the name and contact details of the data protection officer or other contact point where more information can be obtained;
- describe the likely consequences of the personal data breach;
- describe the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

SANCTIONS AND REMEDIES FOR DATA BREACH IN FRANCE

- GDPR guarantees right to an effective remedy (GDPR art. 79); Proceedings against a controller or a processor before the courts of controller or processor's establishment or Data Subject's habitual residence
- Enforcement mechanisms
  - Criminal (typically against perpetrator); powers of police investigation
  - Administrative investigation and enforcement by State DPA (CNIL in France)
  - Civil (no discovery, no legal fees, not punitive damages, but possible EU-wide Group Actions under GDPR Art. 80 (*The data subject shall have the right to mandate a not-for-profit body, organisation or association)*
  - *For outside-EU transfers to USA where inadequate protection: Privacy Shield remedies and arbitration under the FAA.*

EXAMPLES OF BREACH NOTIFICATION SANCTIONS IN FRANCE

1. June 12, 2014, warning against company X (anonymized within 2 years), with public notice of decision (alerted by whistleblower, CNIL admin investigation found data for 600,000 clients available on internet)
2. April 21, 2016, warning and publication against company X (+800 employees) ; despite exclusion of certain parts of Domain from search engine indexing, certain employee personal data available on web. Delegation to vendor does not exonerate company from ensuring compliance;
3. July 18, 2017, Hertz rental cars fined 40K€; customer personal data available through company URLs without any password
4. November 16, 2017, Web Editions fined 25K€ by CNIL; personal data available to public on administrative services site
5. May 7, 2018, Optical Center (retail optician); customer personal data available through various URLs. 250K€ administrative fine.

INVESTIGATIONS IN CIVIL LAW COUNTRIES; BLOCKING STATUTES, PRIVILEGE

- Blocking Statute; the law of 1980 (French criminal prosecution and conviction upheld by French Supreme Court in 2008 in the *Executive Life Insurance* matter, *in re Christopher X*)
- Conflict of jurisdictions and applicable law; *Aérospatiale* 482 U.S. 522 (1987)
- Which law applies to attorney client privilege in multi-jurisdictional investigation (reasons to consult and retain local counsel, even if have in-house counsel available)

ASSESSMENT OF COMPLIANCE REQUIREMENTS AND ENFORCEMENT UNDER GDPR

- Limited history
- Few enforcement actions, civil, criminal or administrative
- Historically financial damages unavailable; under GDPR art. 82 & 83 may now be available but untested

(*Any person who has suffered material or non-material damage as a result of an infringement of this Regulation shall have the right to receive compensation from the controller or processor for the damage suffered*)(*damages up to 20M€ or 4% of world turnover*)

THANK YOU!

Alexander Blumrosen

KAB Avocats, Paris, France