HILGERS | GRABEN

Hilgers Graben PLLC
Data Privacy Compendium & On-Line Desk Book (2016)

Sterling Miller
Senior Counsel
JD, CIPP/US

www.HilgersGraben.com

Introduction[1]

Welcome to the first edition of the Hilgers Graben PLLC *Data Privacy Compendium & On-Line Desk Book* (2016). If you are someone who needs to worry about data privacy and data protection issues (business person, lawyer, etc.), then you already know that this is a constantly evolving area of the law. There is a bewildering amount of material on data privacy and data security available on-line. The challenge for anyone is to read through it all and decide what they think is most useful.

Every year I collect the best materials I can find regarding data privacy and data security and list them in this compendium. There are articles from leading publications, as well as resources available on law firm websites, blogs, and government websites. The idea is to provide readers with a number of helpful materials available *via* hyperlinks directly to the source.

Unless otherwise noted, I take no credit for the materials noted below. These are simply a number of resources that I consider worthy of inclusion in this compendium. There will be a new version for 2017 and I may update or swap out the links below at any time, so always worth checking back from time to time.

Hilgers Graben offers legal counsel and guidance on a number of data privacy and data protection issues, from pre-breach planning to breach support. For more information contact me at smiller@hilgersgraben.com

I also post articles and other materials of interest in this area via the firm's Twitter account and LinkedIn account, so be sure to follow or connect to either or both.

If you have materials you wish for me to consider including in the next edition, please send them to me at the email address above.

Sterling Miller
JD, CIPP/US

January 1, 2016

[1] **No Legal Advice or Attorney-Client Relationship**: This publication has been prepared by Sterling Miller and Hilgers Graben PLLC (together the "firm") for informational purposes and is not legal advice. This publication is not intended to create, and receipt of it does not constitute, a lawyer-client relationship. You should not act upon this publication without seeking advice from a lawyer licensed in your own state or country. Do not send us confidential information until you speak with one of our lawyers and receive our authorization to send that information to us. Providing information to the firm (via e-mail links on this Web site or otherwise) will not create an attorney-client relationship in the absence of an express agreement by the firm to create such a relationship, and will not prevent the firm from representing someone else in connection with the matter in question or a related matter.

No Warranties: This publication, and all information available on or accessed through this publication, is provided "as is." The firm makes no warranties, representations or claims of any kind concerning the information presented on or through this site

Privacy Related Materials

1. Ten Things: Data Privacy Essentials & Ten Things: The New EU Data Privacy Law – What You Really Need to Know (Sterling Miller)
2. Privacy Risk Assessment Questionnaire (IACPA)
3. Guide for Structuring and Implementing Privacy Impact Assessments (TRUSTe)
4. 10 Steps to Mitigate a Data Breach Before it Happens (Arent Fox)
5. Privacy Management Accountability Framework (Nymity)
6. Breach Incident Response: Emergency Preparedness Guide (DLA Piper)
7. Data Security Breaches – Incident Preparedness and Response (Bryan Cave)
8. Data Breach Response Checklist (Practical Law)
9. Data Breach Incident Response Workbook (AllClearID)
10. Security Breach Notification Laws (by State) – 2015 (Weil Gotshal)
11. Global Data Privacy Directory (by country) – 2014 (Norton Rose Fulbright)
12. Social Media Privacy Laws Desk Book – 2015 (Seyfarth Shaw)
13. Verizon 2016 Data Breach Investigations Report (Verizon)
14. NIST Cyber Security Framework (NIST)
15. EU Data Privacy Directive & General Data Privacy Regulation (Final) (EC)
16. Cybersecurity Lexicon for General Counsel (Guidance Software)
17. International Data Transfers (options) (Hogan Lovells)
18. US-EU "Privacy Shield" agreement (Final)
19. Privacy Shield FAQs (Alston)
20. Cyber-insurance: Buyer Beware (10 Tips) (Metro Corporate Counsel)
21. 20 Questions When Your Vendor's Cyber-insurance Matters (John Neiditz)
22. DOJ Best Practices for Victim Response and Reporting of Cyber Incidents (DOJ)

23. Map of Sectorial and Omnibus Privacy/Data Security Laws (Nimity)
24. Introduction to Data Security Breach Preparedness (with model guide) (ABA)
25. Regulatory Investigations Following a Reported Breach (Data Privacy Monitor)
26. You Have a Breach Response Plan … Now How Do You Test It? (Alston/Bird)
27. Data Breach? Top Ten Things to do Next (Sullivan & Worcester)
28. 2015 Cost of Data Breach Study (Ponemon)
29. The Nature of Cyber Risk (Metro Corporate Counsel)
30. Summary of Data Privacy Resources – 2015 (Worldwide ERC)
31. Data Breach Response Guide – (Experian)

Useful Privacy Websites

1. International Association of Privacy Professionals
2. Nymity
3. TRUSTe
4. National Institute of Standards and Technology
5. Article 29 Working Party (EU)
6. Federal Trade Commission – Privacy and Security
7. Ponemon Institute
8. Online Trust Alliance
9. InfraGard

Privacy/Other Blogs

1. Ten Things You Need to Know as In-House Counsel (Sterling Miller)
2. Chronicle of Data Protection (Hogan Lovells)
3. Privacy Matters (DLA Piper)
4. Global Privacy Watch (Seyfarth Shaw)

5. Data Privacy Monitor (Baker Hostetler)
6. Privacy Law Blog (Proskauer Rose)

High Level Data Breach Check List

- Identify the different types of data you have and the levels of protection each require.
  - Implement appropriate physical, technical, and administrative controls.
  - Keep software patches current.
  - Consider the NIST Cybersecurity Framework.
- Ensure you have notified system users (e.g., employees, customers) that you will monitor your systems and their activity as needed to detect and respond to cyber incidents (i.e., via user agreements, workplace policies, training, etc.).
- Engage with law enforcement before there is a breach, i.e., local FBI offices, InfraGard, U.S. Secret Service.
- Have a well-drafted externally facing privacy statement and user agreement. Ensure contracts have appropriate data breach protection language, including data protection compliance obligations in vendor contracts (vet vendors carefully).
- Utilize "Privacy by Design" and "Privacy Impact Assessments."
- Limit the personal data you collect.
- Encrypt personal data and/or consider two-step authentication.
- Have a detailed data breach plan in place before there is an intrusion or breach, including identifying your internal team (including back-ups), contact information, third party help (e.g., outside legal, media expert), forensic plans/vendors, off-site data back-up, and so forth.
  - Practice it.
  - Disseminate it.
  - Update it.
- If there is an incident, put data breach plan into effect immediately.
  - Assemble the contact players (or back-ups) identified in the plan to analyze incident as soon as possible, i.e., within one hour.
- Is this a true data breach (i.e., a loss of personally identifiable data along with SSN#, password, driver's license #, etc.) or just a data incident?
  - Data breach requires more substantive response than an incident. For example, U.S. state notification laws only apply in the event of a data breach, not a data incident.
- If a data breach:
  - Contact: legal counsel, IT forensics specialists, media relations team, and any other appropriate outside vendors.
    - Coordinate work with legal counsel, especially with respect to written materials
  - Quickly assess the situation ("who, what, where, when, why, and how").
    - What systems are affected?
    - What data?
    - Who launched attack?
    - Document everything you can about the breach including what you did and why in response to it
  - Ensure breach has ended and ensure that affected systems are fixed and locked down.

        - Properly preserve evidence (reports, logs, audits, suspicious emails, hacked accounts, etc.)
    - Begin forensic investigation into cause and scope.
        - For example, image the affected computers
    - Determine whether you need to notify law enforcement or state attorneys general.
        - Even if not required, consider with counsel whether such notification makes sense regardless
    - Determine notification obligations (to customers, employees, etc.) and applicable timelines under various laws (state, federal, foreign).
    - Determine if vendors are the (or a) source of the breach.
    - If health care information is involved, understand that additional requirements may apply.
    - Contact insurance company.
    - Monitor company bank accounts and require additional approvals for transfer of sums above a certain amount.
    - Understand any notification obligations under contracts with vendors and customers.
    - Determine, if needed, logistics of a call center (to deal with calls from customers)/notification process – consider hiring a third party vendor to run the operation.
    - Create breach communications plan, internal and external:
        - Media
        - Employees
        - Senior management/Board of Directors
        - Customers
        - Investor relations
        - Regulators/law enforcement
        - Public Affairs
        - Contents of potential apology
- Post breach:
    - Continue to monitor networks/systems to ensure threat was eradicated/stopped.
    - Evaluate effectiveness of data breach plan and response overall.
        - Make changes as needed
    - Update any other relevant internal policies and procedures.
    - Make changes to systems needed to prevent breach from occurring again.
    - Update data security training/awareness for employees, especially employee training around cyber-hygiene (e.g., strong passwords, up-to-date antivirus software and patches, "phishing" training).
    - Cooperate with law enforcement as needed.
    - Improve vendor vetting process.
    - Encrypt data if feasible ("at rest" and "on move").

HILGERS | GRABEN

www.hilgersgraben.com | info@hilgersgraben.com

Follow us on Twitter @HilgersGraben
and on LinkedIn @ Hilgers Graben PLLC

Dallas · Lincoln · Omaha

Litigation | Internal Investigations | Cyber Risk/Data Privacy
Compliance | Discovery Counsel | Trademarks | Copyrights
Legal Project Management