BAKER & MCKENZIE

Datensicherheit & Haftungsrisiko nach der neuen Datenschutzgrundverordnung

RA Dr. Lukas Feiler, SSCP, CIPP/E

Security Forum 2016
20. April 2016

TOPICS

1) Die Datenschutzgrundverordnung (DSGV) im Überblick
2) Datensicherheitspflichten nach der DSGV
3) Prichten zur Offenlegung von Sicherheitsverletzungen
4) Verwaltungsstrafrechtliche Haftung
5) Schadenersatzrechtliche Haftung und „Class Actions“

Die DSGV im Überblick

- Vision: Vollharmonisierung des Datenschutzrechts
- Realität: mehr 20 Regelungszuständigkeiten für Mitgliedstaaten
- Strafen von bis zu 20 Million Euro oder 4% des jährlichen weltweiten Umsatzes
- Interne Dokumentations- und Prüfpflichten statt Meldepflichten
- Betrieblicher Datenschutzbeauftragter
- Auftragsverarbeiter gleichermaßen reguliert
- Hoch komplexe Zuständigkeitsordnung (kein Konzernprivileg)

Datensicherheitspflichten 1 von 3

- Daten sind zu schützen vor
  - Verlust der Vertraulichkeit
  - Verlust der Verfügbarkeit
  - Verlust der Integrität
  - unbefugter oder unrechtmäßiger Verarbeitung
    - → *Rechtmäßigkeit*
- Informationssicherheit nicht ausreichend!

Datensicherheitspflichten 2 von 3

- Risikoangemessene Sicherheitsmaßnahmen unter Berücksichtigung
  - des Stands der Technik,
  - der Implementierungskosten,
  - der Art, Umfangs & Zwecke der Verarbeitung und
  - der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen

    → Risikobewertung & Kosten/Nutzenanalyse erforderlich
- Herausforderung für die Praxis: Quantifizierung des Risikos

Datensicherheitspflichten 3 von 3

- Angemessene Maßnahmen umfassen laut DSGV isnb.:
  - Pseudonymisierung und Verschlüsselung
  - die Fähigkeit, die Sicherheit der Systeme sicherzustellen;
  - die Fähigkeit, Verfügbarkeit nach einem Zwischenfall rasch wiederherzustellen → Incident Response Capabilities;
  - Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der Sicherheitsmaßnahmen → Audits
- Technische Standards ausreichend?
  - z.B. Center for Internet Security Critical Security Controls oder ISO/IEC 27001?

Pflichten zur Offenlegung von Sicherheitsverletzung – 1 von 2

- Offenlegungspflicht, wenn Verletzung von Vertraulichkeit, Verfügbarkeit oder Integrität von personenbezogenen Daten
- Verpflichtende Notifikation an Datenschutzbehörde, wenn
  - Unternehmen Kenntnis von Sicherheitsverletzung erlangt &
  - *Risiko* für die Rechte und Freiheiten natürlicher Personen
- Verpflichtende Notifikation an Betroffene, wenn
  - Unternehmen Kenntnis von Sicherheitsverletzung erlangt &
  - *hohes Risiko* für die persönlichen Rechte und Freiheiten natürlicher Personen
- Notifikationen müssen unverzüglich, an die Behörde möglichst binnen 72 Stunden erfolgen
- Behörde kann Notifikation der Betroffenen anordnen

Pflichten zur Offenlegung von Sicherheitsverletzung – 2 von 2

- Inhalt der Notifikation
  - Namen und die Kontaktdaten des Datenschutzbeauftragten
  - wahrscheinlichen Folgen der Verletzung
  - ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung
- Zustäzlich bei Notifikation an Behörde
  - Kategorien und ungefähre Zahl der Betroffenen
  - Kategorien und ungefähren Zahl der Datensätze

Verwaltungs-strafrechtliche Haftung

- Verletzungen der DSGV werden Sanktioniert mit einer Geldstrafe von bis zu
  - 20 Millionen Euro oder
  - 4% des weltweiten jährlichen Umsatzes

  je nachdem, welcher der Beträge höher ist.
- Haftung der Geschäftsleitung?
  - Grds gilt, dass Mitglieder der Geschäftsleitung solidarisch mit der Gesellschaft haften (§ 9 Verwaltungsstrafgesetz)
  - Ausnahme: Bestellung eines „verantwortlichen Beauftragten“

Schadenersatzrechtliche Haftung

- Jeder Betroffene hat Recht auf Ersatz des
  - materiellen Schadens und
  - immateriellen Schadens (z.B. Diskriminierung od Identitätsdiebstahl)
- Schadenersatzpflicht entfällt, wenn Beklagter beweisen kann, dass es für „den Umstand, durch den der Schaden eingetreten ist, [nicht] verantwortlich ist“ → Beklagte muss sich freibeweisen
- Gerichtsstand: Betroffener kann klagen, wo
  - der Beklagte eine Niederlassung hat oder
  - der Betroffene seinen Aufenthaltsort hat

  → Forum Shopping für Betroffene leicht möglich

Schadenersatzrechtliche Haftung & “Class Actions”

- Mitgliedstaaten können im nationalen Recht vorsehen, dass Betroffene das Recht haben, einer Datenschutzorganisationen ihre Schadenersatzansprüche abzutreten
- Datenschutzorganisation kann so Schadenersatzansprüche tausender Betroffener gebündelt geltend machen
  → „Class Action“
- Gerichtsstand: Datenschutzorganisation kann klagen, wo der Beklagte eine Niederlassung hat
  → Forum Shopping auch für Datenschutzorganisationen möglich

Kontakt

Baker & McKenzie
Schottenring 25
1010 Vienna
Tel.: +43 (0) 1 24 250
Fax: +43 (0) 1 24 250 600

RA Dr. Lukas Feiler, SSCP, CIPP/E
lukas.feiler@bakermckenzie.com

BAKER & MCKENZIE

Datensicherheit & Haftungsrisiko nach der neuen Datenschutzgrundverordnung

RA Dr. Lukas Feiler, SSCP, CIPP/E

Security Forum 2016
20. April 2016

TOPICS

1) Die Datenschutzgrundverordnung (DSGV) im Überblick
2) Datensicherheitspflichten nach der DSGV
3) Prichten zur Offenlegung von Sicherheitsverletzungen
4) Verwaltungsstrafrechtliche Haftung
5) Schadenersatzrechtliche Haftung und „Class Actions“

Die DSGV im Überblick

- Vision: Vollharmonisierung des Datenschutzrechts
- Realität: mehr 20 Regelungszuständigkeiten für Mitgliedstaaten
- Strafen von bis zu 20 Million Euro oder 4% des jährlichen weltweiten Umsatzes
- Interne Dokumentations- und Prüfpflichten statt Meldepflichten
- Betrieblicher Datenschutzbeauftragter
- Auftragsverarbeiter gleichermaßen reguliert
- Hoch komplexe Zuständigkeitsordnung (kein Konzernprivileg)

Datensicherheitspflichten 1 von 3

- Daten sind zu schützen vor
  - Verlust der Vertraulichkeit
  - Verlust der Verfügbarkeit
  - Verlust der Integrität
  - unbefugter oder unrechtmäßiger Verarbeitung
    - → *Rechtmäßigkeit*
- Informationssicherheit nicht ausreichend!

Datensicherheitspflichten 2 von 3

- Risikoangemessene Sicherheitsmaßnahmen unter Berücksichtigung
  - des Stands der Technik,
  - der Implementierungskosten,
  - der Art, Umfangs & Zwecke der Verarbeitung und
  - der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen

    → Risikobewertung & Kosten/Nutzenanalyse erforderlich
- Herausforderung für die Praxis: Quantifizierung des Risikos

Datensicherheitspflichten 3 von 3

- Angemessene Maßnahmen umfassen laut DSGV isnb.:
  - Pseudonymisierung und Verschlüsselung
  - die Fähigkeit, die Sicherheit der Systeme sicherzustellen;
  - die Fähigkeit, Verfügbarkeit nach einem Zwischenfall rasch wiederherzustellen → Incident Response Capabilities;
  - Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der Sicherheitsmaßnahmen → Audits
- Technische Standards ausreichend?
  - z.B. Center for Internet Security Critical Security Controls oder ISO/IEC 27001?

Pflichten zur Offenlegung von Sicherheitsverletzung – 1 von 2

- Offenlegungspflicht, wenn Verletzung von Vertraulichkeit, Verfügbarkeit oder Integrität von personenbezogenen Daten
- Verpflichtende Notifikation an Datenschutzbehörde, wenn
  - Unternehmen Kenntnis von Sicherheitsverletzung erlangt &
  - *Risiko* für die Rechte und Freiheiten natürlicher Personen
- Verpflichtende Notifikation an Betroffene, wenn
  - Unternehmen Kenntnis von Sicherheitsverletzung erlangt &
  - *hohes Risiko* für die persönlichen Rechte und Freiheiten natürlicher Personen
- Notifikationen müssen unverzüglich, an die Behörde möglichst binnen 72 Stunden erfolgen
- Behörde kann Notifikation der Betroffenen anordnen

Pflichten zur Offenlegung von Sicherheitsverletzung – 2 von 2

- Inhalt der Notifikation
  - Namen und die Kontaktdaten des Datenschutzbeauftragten
  - wahrscheinlichen Folgen der Verletzung
  - ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung
- Zustäzlich bei Notifikation an Behörde
  - Kategorien und ungefähre Zahl der Betroffenen
  - Kategorien und ungefähren Zahl der Datensätze

Verwaltungs-strafrechtliche Haftung

- Verletzungen der DSGV werden Sanktioniert mit einer Geldstrafe von bis zu
  - 20 Millionen Euro oder
  - 4% des weltweiten jährlichen Umsatzes

  je nachdem, welcher der Beträge höher ist.
- Haftung der Geschäftsleitung?
  - Grds gilt, dass Mitglieder der Geschäftsleitung solidarisch mit der Gesellschaft haften (§ 9 Verwaltungsstrafgesetz)
  - Ausnahme: Bestellung eines „verantwortlichen Beauftragten“

Schadenersatzrechtliche Haftung

- Jeder Betroffene hat Recht auf Ersatz des
  - materiellen Schadens und
  - immateriellen Schadens (z.B. Diskriminierung od Identitätsdiebstahl)
- Schadenersatzpflicht entfällt, wenn Beklagter beweisen kann, dass es für „den Umstand, durch den der Schaden eingetreten ist, [nicht] verantwortlich ist“ → Beklagte muss sich freibeweisen
- Gerichtsstand: Betroffener kann klagen, wo
  - der Beklagte eine Niederlassung hat oder
  - der Betroffene seinen Aufenthaltsort hat

  → Forum Shopping für Betroffene leicht möglich

Schadenersatzrechtliche Haftung & “Class Actions”

- Mitgliedstaaten können im nationalen Recht vorsehen, dass Betroffene das Recht haben, einer Datenschutzorganisationen ihre Schadenersatzansprüche abzutreten
- Datenschutzorganisation kann so Schadenersatzansprüche tausender Betroffener gebündelt geltend machen
  → „Class Action“
- Gerichtsstand: Datenschutzorganisation kann klagen, wo der Beklagte eine Niederlassung hat
  → Forum Shopping auch für Datenschutzorganisationen möglich

Kontakt

Baker & McKenzie
Schottenring 25
1010 Vienna
Tel.: +43 (0) 1 24 250
Fax: +43 (0) 1 24 250 600

RA Dr. Lukas Feiler, SSCP, CIPP/E
lukas.feiler@bakermckenzie.com

BAKER & MCKENZIE

Datensicherheit & Haftungsrisiko nach der neuen Datenschutzgrundverordnung

RA Dr. Lukas Feiler, SSCP, CIPP/E

Security Forum 2016
20. April 2016

TOPICS

1) Die Datenschutzgrundverordnung (DSGV) im Überblick
2) Datensicherheitspflichten nach der DSGV
3) Prichten zur Offenlegung von Sicherheitsverletzungen
4) Verwaltungsstrafrechtliche Haftung
5) Schadenersatzrechtliche Haftung und „Class Actions“

Die DSGV im Überblick

- Vision: Vollharmonisierung des Datenschutzrechts
- Realität: mehr 20 Regelungszuständigkeiten für Mitgliedstaaten
- Strafen von bis zu 20 Million Euro oder 4% des jährlichen weltweiten Umsatzes
- Interne Dokumentations- und Prüfpflichten statt Meldepflichten
- Betrieblicher Datenschutzbeauftragter
- Auftragsverarbeiter gleichermaßen reguliert
- Hoch komplexe Zuständigkeitsordnung (kein Konzernprivileg)

Datensicherheitspflichten 1 von 3

- Daten sind zu schützen vor
  - Verlust der Vertraulichkeit
  - Verlust der Verfügbarkeit
  - Verlust der Integrität
  - unbefugter oder unrechtmäßiger Verarbeitung
    - → *Rechtmäßigkeit*
- Informationssicherheit nicht ausreichend!

Datensicherheitspflichten 2 von 3

- Risikoangemessene Sicherheitsmaßnahmen unter Berücksichtigung
  - des Stands der Technik,
  - der Implementierungskosten,
  - der Art, Umfangs & Zwecke der Verarbeitung und
  - der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen

    → Risikobewertung & Kosten/Nutzenanalyse erforderlich
- Herausforderung für die Praxis: Quantifizierung des Risikos

Datensicherheitspflichten 3 von 3

- Angemessene Maßnahmen umfassen laut DSGV isnb.:
  - Pseudonymisierung und Verschlüsselung
  - die Fähigkeit, die Sicherheit der Systeme sicherzustellen;
  - die Fähigkeit, Verfügbarkeit nach einem Zwischenfall rasch wiederherzustellen → Incident Response Capabilities;
  - Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der Sicherheitsmaßnahmen → Audits
- Technische Standards ausreichend?
  - z.B. Center for Internet Security Critical Security Controls oder ISO/IEC 27001?

Pflichten zur Offenlegung von Sicherheitsverletzung – 1 von 2

- Offenlegungspflicht, wenn Verletzung von Vertraulichkeit, Verfügbarkeit oder Integrität von personenbezogenen Daten
- Verpflichtende Notifikation an Datenschutzbehörde, wenn
  - Unternehmen Kenntnis von Sicherheitsverletzung erlangt &
  - *Risiko* für die Rechte und Freiheiten natürlicher Personen
- Verpflichtende Notifikation an Betroffene, wenn
  - Unternehmen Kenntnis von Sicherheitsverletzung erlangt &
  - *hohes Risiko* für die persönlichen Rechte und Freiheiten natürlicher Personen
- Notifikationen müssen unverzüglich, an die Behörde möglichst binnen 72 Stunden erfolgen
- Behörde kann Notifikation der Betroffenen anordnen

Pflichten zur Offenlegung von Sicherheitsverletzung – 2 von 2

- Inhalt der Notifikation
  - Namen und die Kontaktdaten des Datenschutzbeauftragten
  - wahrscheinlichen Folgen der Verletzung
  - ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung
- Zustäzlich bei Notifikation an Behörde
  - Kategorien und ungefähre Zahl der Betroffenen
  - Kategorien und ungefähren Zahl der Datensätze

Verwaltungs-strafrechtliche Haftung

- Verletzungen der DSGV werden Sanktioniert mit einer Geldstrafe von bis zu
  - 20 Millionen Euro oder
  - 4% des weltweiten jährlichen Umsatzes

  je nachdem, welcher der Beträge höher ist.
- Haftung der Geschäftsleitung?
  - Grds gilt, dass Mitglieder der Geschäftsleitung solidarisch mit der Gesellschaft haften (§ 9 Verwaltungsstrafgesetz)
  - Ausnahme: Bestellung eines „verantwortlichen Beauftragten“

Schadenersatzrechtliche Haftung

- Jeder Betroffene hat Recht auf Ersatz des
  - materiellen Schadens und
  - immateriellen Schadens (z.B. Diskriminierung od Identitätsdiebstahl)
- Schadenersatzpflicht entfällt, wenn Beklagter beweisen kann, dass es für „den Umstand, durch den der Schaden eingetreten ist, [nicht] verantwortlich ist“ → Beklagte muss sich freibeweisen
- Gerichtsstand: Betroffener kann klagen, wo
  - der Beklagte eine Niederlassung hat oder
  - der Betroffene seinen Aufenthaltsort hat

  → Forum Shopping für Betroffene leicht möglich

Schadenersatzrechtliche Haftung & “Class Actions”

- Mitgliedstaaten können im nationalen Recht vorsehen, dass Betroffene das Recht haben, einer Datenschutzorganisationen ihre Schadenersatzansprüche abzutreten
- Datenschutzorganisation kann so Schadenersatzansprüche tausender Betroffener gebündelt geltend machen
  → „Class Action“
- Gerichtsstand: Datenschutzorganisation kann klagen, wo der Beklagte eine Niederlassung hat
  → Forum Shopping auch für Datenschutzorganisationen möglich

Kontakt

Baker & McKenzie
Schottenring 25
1010 Vienna
Tel.: +43 (0) 1 24 250
Fax: +43 (0) 1 24 250 600

RA Dr. Lukas Feiler, SSCP, CIPP/E
lukas.feiler@bakermckenzie.com

BAKER & MCKENZIE

Datensicherheit & Haftungsrisiko nach der neuen Datenschutzgrundverordnung

RA Dr. Lukas Feiler, SSCP, CIPP/E

Security Forum 2016
20. April 2016

TOPICS

1) Die Datenschutzgrundverordnung (DSGV) im Überblick
2) Datensicherheitspflichten nach der DSGV
3) Prichten zur Offenlegung von Sicherheitsverletzungen
4) Verwaltungsstrafrechtliche Haftung
5) Schadenersatzrechtliche Haftung und „Class Actions“

Die DSGV im Überblick

- Vision: Vollharmonisierung des Datenschutzrechts
- Realität: mehr 20 Regelungszuständigkeiten für Mitgliedstaaten
- Strafen von bis zu 20 Million Euro oder 4% des jährlichen weltweiten Umsatzes
- Interne Dokumentations- und Prüfpflichten statt Meldepflichten
- Betrieblicher Datenschutzbeauftragter
- Auftragsverarbeiter gleichermaßen reguliert
- Hoch komplexe Zuständigkeitsordnung (kein Konzernprivileg)

Datensicherheitspflichten 1 von 3

- Daten sind zu schützen vor
  - Verlust der Vertraulichkeit
  - Verlust der Verfügbarkeit
  - Verlust der Integrität
  - unbefugter oder unrechtmäßiger Verarbeitung
    - → *Rechtmäßigkeit*
- Informationssicherheit nicht ausreichend!

Datensicherheitspflichten 2 von 3

- Risikoangemessene Sicherheitsmaßnahmen unter Berücksichtigung
  - des Stands der Technik,
  - der Implementierungskosten,
  - der Art, Umfangs & Zwecke der Verarbeitung und
  - der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen

    → Risikobewertung & Kosten/Nutzenanalyse erforderlich
- Herausforderung für die Praxis: Quantifizierung des Risikos

Datensicherheitspflichten 3 von 3

- Angemessene Maßnahmen umfassen laut DSGV isnb.:
  - Pseudonymisierung und Verschlüsselung
  - die Fähigkeit, die Sicherheit der Systeme sicherzustellen;
  - die Fähigkeit, Verfügbarkeit nach einem Zwischenfall rasch wiederherzustellen → Incident Response Capabilities;
  - Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der Sicherheitsmaßnahmen → Audits
- Technische Standards ausreichend?
  - z.B. Center for Internet Security Critical Security Controls oder ISO/IEC 27001?

Pflichten zur Offenlegung von Sicherheitsverletzung – 1 von 2

- Offenlegungspflicht, wenn Verletzung von Vertraulichkeit, Verfügbarkeit oder Integrität von personenbezogenen Daten
- Verpflichtende Notifikation an Datenschutzbehörde, wenn
  - Unternehmen Kenntnis von Sicherheitsverletzung erlangt &
  - *Risiko* für die Rechte und Freiheiten natürlicher Personen
- Verpflichtende Notifikation an Betroffene, wenn
  - Unternehmen Kenntnis von Sicherheitsverletzung erlangt &
  - *hohes Risiko* für die persönlichen Rechte und Freiheiten natürlicher Personen
- Notifikationen müssen unverzüglich, an die Behörde möglichst binnen 72 Stunden erfolgen
- Behörde kann Notifikation der Betroffenen anordnen

Pflichten zur Offenlegung von Sicherheitsverletzung – 2 von 2

- Inhalt der Notifikation
  - Namen und die Kontaktdaten des Datenschutzbeauftragten
  - wahrscheinlichen Folgen der Verletzung
  - ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung
- Zustäzlich bei Notifikation an Behörde
  - Kategorien und ungefähre Zahl der Betroffenen
  - Kategorien und ungefähren Zahl der Datensätze

Verwaltungs-strafrechtliche Haftung

- Verletzungen der DSGV werden Sanktioniert mit einer Geldstrafe von bis zu
  - 20 Millionen Euro oder
  - 4% des weltweiten jährlichen Umsatzes

  je nachdem, welcher der Beträge höher ist.
- Haftung der Geschäftsleitung?
  - Grds gilt, dass Mitglieder der Geschäftsleitung solidarisch mit der Gesellschaft haften (§ 9 Verwaltungsstrafgesetz)
  - Ausnahme: Bestellung eines „verantwortlichen Beauftragten“

Schadenersatzrechtliche Haftung

- Jeder Betroffene hat Recht auf Ersatz des
  - materiellen Schadens und
  - immateriellen Schadens (z.B. Diskriminierung od Identitätsdiebstahl)
- Schadenersatzpflicht entfällt, wenn Beklagter beweisen kann, dass es für „den Umstand, durch den der Schaden eingetreten ist, [nicht] verantwortlich ist“ → Beklagte muss sich freibeweisen
- Gerichtsstand: Betroffener kann klagen, wo
  - der Beklagte eine Niederlassung hat oder
  - der Betroffene seinen Aufenthaltsort hat

  → Forum Shopping für Betroffene leicht möglich

Schadenersatzrechtliche Haftung & “Class Actions”

- Mitgliedstaaten können im nationalen Recht vorsehen, dass Betroffene das Recht haben, einer Datenschutzorganisationen ihre Schadenersatzansprüche abzutreten
- Datenschutzorganisation kann so Schadenersatzansprüche tausender Betroffener gebündelt geltend machen
  → „Class Action“
- Gerichtsstand: Datenschutzorganisation kann klagen, wo der Beklagte eine Niederlassung hat
  → Forum Shopping auch für Datenschutzorganisationen möglich

Kontakt

Baker & McKenzie
Schottenring 25
1010 Vienna
Tel.: +43 (0) 1 24 250
Fax: +43 (0) 1 24 250 600

RA Dr. Lukas Feiler, SSCP, CIPP/E
lukas.feiler@bakermckenzie.com

BAKER & MCKENZIE

Datensicherheit & Haftungsrisiko nach der neuen Datenschutzgrundverordnung

RA Dr. Lukas Feiler, SSCP, CIPP/E

Security Forum 2016
20. April 2016

TOPICS

1) Die Datenschutzgrundverordnung (DSGV) im Überblick
2) Datensicherheitspflichten nach der DSGV
3) Prichten zur Offenlegung von Sicherheitsverletzungen
4) Verwaltungsstrafrechtliche Haftung
5) Schadenersatzrechtliche Haftung und „Class Actions“

Die DSGV im Überblick

- Vision: Vollharmonisierung des Datenschutzrechts
- Realität: mehr 20 Regelungszuständigkeiten für Mitgliedstaaten
- Strafen von bis zu 20 Million Euro oder 4% des jährlichen weltweiten Umsatzes
- Interne Dokumentations- und Prüfpflichten statt Meldepflichten
- Betrieblicher Datenschutzbeauftragter
- Auftragsverarbeiter gleichermaßen reguliert
- Hoch komplexe Zuständigkeitsordnung (kein Konzernprivileg)

Datensicherheitspflichten 1 von 3

- Daten sind zu schützen vor
  - Verlust der Vertraulichkeit
  - Verlust der Verfügbarkeit
  - Verlust der Integrität
  - unbefugter oder unrechtmäßiger Verarbeitung
    - → *Rechtmäßigkeit*
- Informationssicherheit nicht ausreichend!

Datensicherheitspflichten 2 von 3

- Risikoangemessene Sicherheitsmaßnahmen unter Berücksichtigung
  - des Stands der Technik,
  - der Implementierungskosten,
  - der Art, Umfangs & Zwecke der Verarbeitung und
  - der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen

    → Risikobewertung & Kosten/Nutzenanalyse erforderlich
- Herausforderung für die Praxis: Quantifizierung des Risikos

Datensicherheitspflichten 3 von 3

- Angemessene Maßnahmen umfassen laut DSGV isnb.:
  - Pseudonymisierung und Verschlüsselung
  - die Fähigkeit, die Sicherheit der Systeme sicherzustellen;
  - die Fähigkeit, Verfügbarkeit nach einem Zwischenfall rasch wiederherzustellen → Incident Response Capabilities;
  - Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der Sicherheitsmaßnahmen → Audits
- Technische Standards ausreichend?
  - z.B. Center for Internet Security Critical Security Controls oder ISO/IEC 27001?

Pflichten zur Offenlegung von Sicherheitsverletzung – 1 von 2

- Offenlegungspflicht, wenn Verletzung von Vertraulichkeit, Verfügbarkeit oder Integrität von personenbezogenen Daten
- Verpflichtende Notifikation an Datenschutzbehörde, wenn
  - Unternehmen Kenntnis von Sicherheitsverletzung erlangt &
  - *Risiko* für die Rechte und Freiheiten natürlicher Personen
- Verpflichtende Notifikation an Betroffene, wenn
  - Unternehmen Kenntnis von Sicherheitsverletzung erlangt &
  - *hohes Risiko* für die persönlichen Rechte und Freiheiten natürlicher Personen
- Notifikationen müssen unverzüglich, an die Behörde möglichst binnen 72 Stunden erfolgen
- Behörde kann Notifikation der Betroffenen anordnen

Pflichten zur Offenlegung von Sicherheitsverletzung – 2 von 2

- Inhalt der Notifikation
  - Namen und die Kontaktdaten des Datenschutzbeauftragten
  - wahrscheinlichen Folgen der Verletzung
  - ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung
- Zustäzlich bei Notifikation an Behörde
  - Kategorien und ungefähre Zahl der Betroffenen
  - Kategorien und ungefähren Zahl der Datensätze

Verwaltungs-strafrechtliche Haftung

- Verletzungen der DSGV werden Sanktioniert mit einer Geldstrafe von bis zu
  - 20 Millionen Euro oder
  - 4% des weltweiten jährlichen Umsatzes

  je nachdem, welcher der Beträge höher ist.
- Haftung der Geschäftsleitung?
  - Grds gilt, dass Mitglieder der Geschäftsleitung solidarisch mit der Gesellschaft haften (§ 9 Verwaltungsstrafgesetz)
  - Ausnahme: Bestellung eines „verantwortlichen Beauftragten“

Schadenersatzrechtliche Haftung

- Jeder Betroffene hat Recht auf Ersatz des
  - materiellen Schadens und
  - immateriellen Schadens (z.B. Diskriminierung od Identitätsdiebstahl)
- Schadenersatzpflicht entfällt, wenn Beklagter beweisen kann, dass es für „den Umstand, durch den der Schaden eingetreten ist, [nicht] verantwortlich ist“ → Beklagte muss sich freibeweisen
- Gerichtsstand: Betroffener kann klagen, wo
  - der Beklagte eine Niederlassung hat oder
  - der Betroffene seinen Aufenthaltsort hat

  → Forum Shopping für Betroffene leicht möglich

Schadenersatzrechtliche Haftung & “Class Actions”

- Mitgliedstaaten können im nationalen Recht vorsehen, dass Betroffene das Recht haben, einer Datenschutzorganisationen ihre Schadenersatzansprüche abzutreten
- Datenschutzorganisation kann so Schadenersatzansprüche tausender Betroffener gebündelt geltend machen
  → „Class Action“
- Gerichtsstand: Datenschutzorganisation kann klagen, wo der Beklagte eine Niederlassung hat
  → Forum Shopping auch für Datenschutzorganisationen möglich

Kontakt

Baker & McKenzie
Schottenring 25
1010 Vienna
Tel.: +43 (0) 1 24 250
Fax: +43 (0) 1 24 250 600

RA Dr. Lukas Feiler, SSCP, CIPP/E
lukas.feiler@bakermckenzie.com

BAKER & MCKENZIE

Datensicherheit & Haftungsrisiko nach der neuen Datenschutzgrundverordnung

RA Dr. Lukas Feiler, SSCP, CIPP/E

Security Forum 2016
20. April 2016

TOPICS

1) Die Datenschutzgrundverordnung (DSGV) im Überblick
2) Datensicherheitspflichten nach der DSGV
3) Prichten zur Offenlegung von Sicherheitsverletzungen
4) Verwaltungsstrafrechtliche Haftung
5) Schadenersatzrechtliche Haftung und „Class Actions“

Die DSGV im Überblick

- Vision: Vollharmonisierung des Datenschutzrechts
- Realität: mehr 20 Regelungszuständigkeiten für Mitgliedstaaten
- Strafen von bis zu 20 Million Euro oder 4% des jährlichen weltweiten Umsatzes
- Interne Dokumentations- und Prüfpflichten statt Meldepflichten
- Betrieblicher Datenschutzbeauftragter
- Auftragsverarbeiter gleichermaßen reguliert
- Hoch komplexe Zuständigkeitsordnung (kein Konzernprivileg)

Datensicherheitspflichten 1 von 3

- Daten sind zu schützen vor
  - Verlust der Vertraulichkeit
  - Verlust der Verfügbarkeit
  - Verlust der Integrität
  - unbefugter oder unrechtmäßiger Verarbeitung
    - → *Rechtmäßigkeit*
- Informationssicherheit nicht ausreichend!

Datensicherheitspflichten 2 von 3

- Risikoangemessene Sicherheitsmaßnahmen unter Berücksichtigung
  - des Stands der Technik,
  - der Implementierungskosten,
  - der Art, Umfangs & Zwecke der Verarbeitung und
  - der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen

    → Risikobewertung & Kosten/Nutzenanalyse erforderlich
- Herausforderung für die Praxis: Quantifizierung des Risikos

Datensicherheitspflichten 3 von 3

- Angemessene Maßnahmen umfassen laut DSGV isnb.:
  - Pseudonymisierung und Verschlüsselung
  - die Fähigkeit, die Sicherheit der Systeme sicherzustellen;
  - die Fähigkeit, Verfügbarkeit nach einem Zwischenfall rasch wiederherzustellen → Incident Response Capabilities;
  - Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der Sicherheitsmaßnahmen → Audits
- Technische Standards ausreichend?
  - z.B. Center for Internet Security Critical Security Controls oder ISO/IEC 27001?

Pflichten zur Offenlegung von Sicherheitsverletzung – 1 von 2

- Offenlegungspflicht, wenn Verletzung von Vertraulichkeit, Verfügbarkeit oder Integrität von personenbezogenen Daten
- Verpflichtende Notifikation an Datenschutzbehörde, wenn
  - Unternehmen Kenntnis von Sicherheitsverletzung erlangt &
  - *Risiko* für die Rechte und Freiheiten natürlicher Personen
- Verpflichtende Notifikation an Betroffene, wenn
  - Unternehmen Kenntnis von Sicherheitsverletzung erlangt &
  - *hohes Risiko* für die persönlichen Rechte und Freiheiten natürlicher Personen
- Notifikationen müssen unverzüglich, an die Behörde möglichst binnen 72 Stunden erfolgen
- Behörde kann Notifikation der Betroffenen anordnen

Pflichten zur Offenlegung von Sicherheitsverletzung – 2 von 2

- Inhalt der Notifikation
  - Namen und die Kontaktdaten des Datenschutzbeauftragten
  - wahrscheinlichen Folgen der Verletzung
  - ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung
- Zustäzlich bei Notifikation an Behörde
  - Kategorien und ungefähre Zahl der Betroffenen
  - Kategorien und ungefähren Zahl der Datensätze

Verwaltungs-strafrechtliche Haftung

- Verletzungen der DSGV werden Sanktioniert mit einer Geldstrafe von bis zu
  - 20 Millionen Euro oder
  - 4% des weltweiten jährlichen Umsatzes

  je nachdem, welcher der Beträge höher ist.
- Haftung der Geschäftsleitung?
  - Grds gilt, dass Mitglieder der Geschäftsleitung solidarisch mit der Gesellschaft haften (§ 9 Verwaltungsstrafgesetz)
  - Ausnahme: Bestellung eines „verantwortlichen Beauftragten“

Schadenersatzrechtliche Haftung

- Jeder Betroffene hat Recht auf Ersatz des
  - materiellen Schadens und
  - immateriellen Schadens (z.B. Diskriminierung od Identitätsdiebstahl)
- Schadenersatzpflicht entfällt, wenn Beklagter beweisen kann, dass es für „den Umstand, durch den der Schaden eingetreten ist, [nicht] verantwortlich ist“ → Beklagte muss sich freibeweisen
- Gerichtsstand: Betroffener kann klagen, wo
  - der Beklagte eine Niederlassung hat oder
  - der Betroffene seinen Aufenthaltsort hat

  → Forum Shopping für Betroffene leicht möglich

Schadenersatzrechtliche Haftung & “Class Actions”

- Mitgliedstaaten können im nationalen Recht vorsehen, dass Betroffene das Recht haben, einer Datenschutzorganisationen ihre Schadenersatzansprüche abzutreten
- Datenschutzorganisation kann so Schadenersatzansprüche tausender Betroffener gebündelt geltend machen
  → „Class Action“
- Gerichtsstand: Datenschutzorganisation kann klagen, wo der Beklagte eine Niederlassung hat
  → Forum Shopping auch für Datenschutzorganisationen möglich

Kontakt

Baker & McKenzie
Schottenring 25
1010 Vienna
Tel.: +43 (0) 1 24 250
Fax: +43 (0) 1 24 250 600

RA Dr. Lukas Feiler, SSCP, CIPP/E
lukas.feiler@bakermckenzie.com

BAKER & MCKENZIE

Datensicherheit & Haftungsrisiko nach der neuen Datenschutzgrundverordnung

RA Dr. Lukas Feiler, SSCP, CIPP/E

Security Forum 2016
20. April 2016

TOPICS

1) Die Datenschutzgrundverordnung (DSGV) im Überblick
2) Datensicherheitspflichten nach der DSGV
3) Prichten zur Offenlegung von Sicherheitsverletzungen
4) Verwaltungsstrafrechtliche Haftung
5) Schadenersatzrechtliche Haftung und „Class Actions“

Die DSGV im Überblick

- Vision: Vollharmonisierung des Datenschutzrechts
- Realität: mehr 20 Regelungszuständigkeiten für Mitgliedstaaten
- Strafen von bis zu 20 Million Euro oder 4% des jährlichen weltweiten Umsatzes
- Interne Dokumentations- und Prüfpflichten statt Meldepflichten
- Betrieblicher Datenschutzbeauftragter
- Auftragsverarbeiter gleichermaßen reguliert
- Hoch komplexe Zuständigkeitsordnung (kein Konzernprivileg)

Datensicherheitspflichten 1 von 3

- Daten sind zu schützen vor
  - Verlust der Vertraulichkeit
  - Verlust der Verfügbarkeit
  - Verlust der Integrität
  - unbefugter oder unrechtmäßiger Verarbeitung
    - → *Rechtmäßigkeit*
- Informationssicherheit nicht ausreichend!

Datensicherheitspflichten 2 von 3

- Risikoangemessene Sicherheitsmaßnahmen unter Berücksichtigung
  - des Stands der Technik,
  - der Implementierungskosten,
  - der Art, Umfangs & Zwecke der Verarbeitung und
  - der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen

    → Risikobewertung & Kosten/Nutzenanalyse erforderlich
- Herausforderung für die Praxis: Quantifizierung des Risikos

Datensicherheitspflichten 3 von 3

- Angemessene Maßnahmen umfassen laut DSGV isnb.:
  - Pseudonymisierung und Verschlüsselung
  - die Fähigkeit, die Sicherheit der Systeme sicherzustellen;
  - die Fähigkeit, Verfügbarkeit nach einem Zwischenfall rasch wiederherzustellen → Incident Response Capabilities;
  - Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der Sicherheitsmaßnahmen → Audits
- Technische Standards ausreichend?
  - z.B. Center for Internet Security Critical Security Controls oder ISO/IEC 27001?

Pflichten zur Offenlegung von Sicherheitsverletzung – 1 von 2

- Offenlegungspflicht, wenn Verletzung von Vertraulichkeit, Verfügbarkeit oder Integrität von personenbezogenen Daten
- Verpflichtende Notifikation an Datenschutzbehörde, wenn
  - Unternehmen Kenntnis von Sicherheitsverletzung erlangt &
  - *Risiko* für die Rechte und Freiheiten natürlicher Personen
- Verpflichtende Notifikation an Betroffene, wenn
  - Unternehmen Kenntnis von Sicherheitsverletzung erlangt &
  - *hohes Risiko* für die persönlichen Rechte und Freiheiten natürlicher Personen
- Notifikationen müssen unverzüglich, an die Behörde möglichst binnen 72 Stunden erfolgen
- Behörde kann Notifikation der Betroffenen anordnen

Pflichten zur Offenlegung von Sicherheitsverletzung – 2 von 2

- Inhalt der Notifikation
  - Namen und die Kontaktdaten des Datenschutzbeauftragten
  - wahrscheinlichen Folgen der Verletzung
  - ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung
- Zustäzlich bei Notifikation an Behörde
  - Kategorien und ungefähre Zahl der Betroffenen
  - Kategorien und ungefähren Zahl der Datensätze

Verwaltungs-strafrechtliche Haftung

- Verletzungen der DSGV werden Sanktioniert mit einer Geldstrafe von bis zu
  - 20 Millionen Euro oder
  - 4% des weltweiten jährlichen Umsatzes

  je nachdem, welcher der Beträge höher ist.
- Haftung der Geschäftsleitung?
  - Grds gilt, dass Mitglieder der Geschäftsleitung solidarisch mit der Gesellschaft haften (§ 9 Verwaltungsstrafgesetz)
  - Ausnahme: Bestellung eines „verantwortlichen Beauftragten“

Schadenersatzrechtliche Haftung

- Jeder Betroffene hat Recht auf Ersatz des
  - materiellen Schadens und
  - immateriellen Schadens (z.B. Diskriminierung od Identitätsdiebstahl)
- Schadenersatzpflicht entfällt, wenn Beklagter beweisen kann, dass es für „den Umstand, durch den der Schaden eingetreten ist, [nicht] verantwortlich ist“ → Beklagte muss sich freibeweisen
- Gerichtsstand: Betroffener kann klagen, wo
  - der Beklagte eine Niederlassung hat oder
  - der Betroffene seinen Aufenthaltsort hat

  → Forum Shopping für Betroffene leicht möglich

Schadenersatzrechtliche Haftung & “Class Actions”

- Mitgliedstaaten können im nationalen Recht vorsehen, dass Betroffene das Recht haben, einer Datenschutzorganisationen ihre Schadenersatzansprüche abzutreten
- Datenschutzorganisation kann so Schadenersatzansprüche tausender Betroffener gebündelt geltend machen
  → „Class Action“
- Gerichtsstand: Datenschutzorganisation kann klagen, wo der Beklagte eine Niederlassung hat
  → Forum Shopping auch für Datenschutzorganisationen möglich

Kontakt

Baker & McKenzie
Schottenring 25
1010 Vienna
Tel.: +43 (0) 1 24 250
Fax: +43 (0) 1 24 250 600

RA Dr. Lukas Feiler, SSCP, CIPP/E
lukas.feiler@bakermckenzie.com