독일의 개인정보유출에 따른 법적 대응에 관한 법제

Ⅰ. 개인정보유출 실태

오늘날 거의 모든 국가에서 개인정보를 법으로 보호하고 있다. 그만큼 개인정보가 가지는 의미가 크기 때문이다. 이러한 개인정보가 특히 정보주체의 동의 없이 유출되면 그 사회적 비용은 상당히 높다. 따라서 개인정보가 유출되는 경우 국가는 이에 따른 법적 조치도 함께 규정하고 있다.

독일의 경우에도 개인정보 유출 사례는 날로 증가하고 있다. 연방정보보호위원회는 2011년 8월 31일 언론보도용 공지를 통하여 2009년 9월 1일부터 시행된 개인정보유출시 통지의무에 의해서 연방 및 각 주의 정보보호위원회에 통지된 건수는 약 90개로 집계되었다고 보고하고 있다.[1] 하지만 기업체가 개인정보유출의 통지를 꺼려하기 때문에 실제로는 이보다 훨씬 많을 것이라고 한다.[2] 90개 중에서 상당수는 주로 노트북과 USB 칩과 같은 이동 저장매체의 절도나 분실 그리고 전자우편이나 우편물을 잘못 발송하는 경우였다고 한다. 이 외에 스키밍에 의한 은행정보의 탐지와 해킹을 통한 데이터의 분실도 있고, 건강정보와 같은 특별히 민감한 정보도 있다고 한다. 또한 바덴뷔르텐베르크주의 2010/2011 개인정보보호위원회의 활동보고서에 따르면 지금까지 약 50개의 데이터보호침해가 신고되었다고 한다. 주로 컴퓨터, 노트북, USB 스틱과 같은 저장매체의 분실, 전자우편이나 팩스의 잘못된 발

1) http://www.bfdi.bund.de/DE/Oeffentlichkeitsarbeit/Pressemitteilungen/2011/30_InformationspflichtBeiDatenpannen.html.

2) 대표적인 개인정보유출 사례로는 온라인 숍 네커만(Neckermann)의 게임참여자 정보 유출(2011.5.26), 슈퍼마켓 체인점, 슐레커의 고객정보 유출(2010. 8), 쇼셜네트워크서비스 슐러(Soziales Netzwerk SchülerVZ) 개인정보복제(2009.10.17), 베를린주은행의 신용카드 정보 도난 사건(2008. 12.12), Deutsche Telekom의 고객 정보 유출 사건(2006.4, 2007. 3, 2007. 9, 2008. 11) 등이 있다.

송, 웹사이트의 해킹 등이 원인이었다고 한다.[3]

2010년 한 연구보고서[4]에 따르면 독일에서 발생한 개인정보유출로 인한 평균 비용은 대략 2008년 240만 유로, 2009년 260만유로, 2010년 340만유로 정도라고 한다. 특히 정보 유출이 외부로 알려지는 경우 해당 사업체의 이미지에 손상을 입게 되므로 이를 외부에 알리는 것을 꺼려한다고 한다. 하지만 개인정보를 취급하는 기업체나 국가기관이 개인정보의 유출을 알리지 않는 경우 이를 모르는 정보주체가 입어야 할 손해는 가늠할 수 없을 만큼 클 수도 있기 때문에 정보유출이 있는 경우 일정한 법적 통제가 필요하다.

Ⅱ. 개인정보유출 관련 법제 개관

독일은 연방 및 각 주 차원에서 개인정보유출에 따른 신고의무를 개별 법률에 규정하고 있다. 연방의 경우 2009년 9월 1일부터 연방정보보호법(BDSG), 전기통신법(TKG), 텔레미디어법(TMG)에서 이러한 규정을 두고 있다. 이 규정은 개인정보 유출시 해당 업체가 관할기관과 피해자에게 이를 통지하도록 하여 더 큰 피해를 방지하기 위한 책임기관의 통지의무를 부과한 것이다. 이러한 통지의무를 이행하지 않는 경우 과태료를 부과하며, 중대한 경우에는 형벌로 규제하고 있다. 이들 법률 규정 중 연방정보보호법(BDSG)이 기본 규정이고, 전기통신법(TKG)과 텔레미디어법(TMG)은 전기통신과 정보통신에 있어서 각각 적용되는 특별법이다. 특히 전기통신법은 2011년 12월 22일 개정되어 통신사업자의 정보유출에 대한 보다 강화된 내용을 담고 있다.

한편 각 주는 주의 정보보호법에서 연방정보보호법의 규정들을 준용하거나 독자적인 규정을 두고 있다. 특히 독자적인 규정을 두고 있는 주 법률은 2011년 2월 2일 정보보호법을 개정한 베를린주 정보보호법이다. 베를린주는 이 개정에서 정보유출의 경우 책임기관의 통지의무를 비공공기관뿐만 아니라 베를린주 내의 모든 공공기관으로 확대한 독일에서의 첫 법제로 기록되고 있다.

Ⅲ. 개별적 법제

1. 연방정보보호법(BDSG)

연방정보보호법 제42a조[5]는 개인정보가 타인에 의해서 부당하게 인지된 경우에 통지책임자

3) 30. Tätigkeitsberichte des LfD Baden-Würtenberg, p. 23.

4) Ponemon Institute, 2010 Annual Study : German Cost of a Data Breach, p.12(http://www.symantec.com/content/de/de/about/downloads/press/2010_annual_study.pdf).

5) 연방정보보호법 제42a조 (1) 연방정보보호법 제2조 제4항의 비공공기관 또는 제27조 제1항 제1문 제2호에 의한 공공기관은, 자신들에게 저장되어 있는 다음 각 호의 정보가 제3자에게 부당하게 전달되거나 그 밖의 다른 방법으로 제3자에게 부

가 감독기관과 관련 당사자에게 이를 통지하도록 하는 규정을 두고 있다.

1) 통지의무자: 사기업체 및 공법상 기업체

통지의무자는 비공공기관(제2조 제4항)과 공법상의 기업(제27조 제1항)이다(연방정보보호법 제42a조 제1문). 비공공기관이란 자연인, 법인, 사법상의 회사 및 그 밖의 인적 단체를 말한다. 비공공기관은 공공기관의 직무를 수행하지 않아야 한다. 따라서 비공공기관이 연방이나 각 주의 공공기관의 업무를 수행하게 되는 경우 공공기관에 관한 규정이 적용되어 통지의무자가 아니다(제2조 제4항).

또한, 공법상 기업으로서 경쟁에 참여하는 연방의 공공기관도 통지의무자에 해당한다. 경쟁기업으로 활동하는 각 주의 공공기관은 해당 주의 정보보호법이 연방정보보호법 제42a조를 준용하는 경우에 한해서만 통지의무자에 해당한다. 그러나 현재 모든 주가 연방정보보호법 및 제42a조를 포함한 개별 규정들을 준용하고 있기 때문에 이 규정은 예외없이 경쟁업체로서 활동하는 각 주의 공공기관에도 적용된다.

그 밖의 연방 및 각 주의 공공기관에 대해서는 제42a조가 적용되지 않는다. 이에 대해서 연방정보보호위원회는 공공기관에도 이 규정의 적용을 확대할 것을 요청하고 있다.[6] 특히 세관 서버에 대한 해커공격이 있은 이후 이에 대한 요구가 지지를 받고 있다. 이와 관련하여 이미 2008년 11월 6-7일 양일간 열린 연방 및 각 주 정보보호위원회 제76차 콘퍼런스에서 채택한 결정에서 정보유출시 통지의무자의 투명성을 높일 것을 연방정보보호법의 개정시에 요청한 바 있다.[7]

이와는 달리 연방정보보호법 제42a조의 통지

당하게 인지되어 당사자의 권리나 보호이익이 중대하게 침해될 우려가 있다는 것을 확인한 경우에는 제2문 및 제5문에 의해서 지체 없이 관할기관과 당사자에게 이를 통지하여야 한다. 1. 특별한 종류의 개인정보(제3조 제9항), 2. 직무상 비밀에 속하는 개인정보, 3. 가벌적 행위나 질서위반행위 또는 이들 행위의 혐의와 관련이 있는 개인정보, 4. 은행계좌 및 신용카드계좌에 대한 개인 정보(제1문). 데이터 확보를 위한 적절한 조치가 취해졌거나 지체 없이 취해지지 않은 즉시 그리고 형사소추가 더 이상 위태롭게 되지 않는 즉시 지체 없이 당사자에게 통지되어야 한다(제2문). 당사자에 대한 통지에는 부당하게 인지된 방법의 설명과 예상되는 불리한 결과를 최소화하기 위한 조치의 추천이 포함되어야 한다(제3문). 관할감독기관에 대한 통지는 이 외에 부당한 인지로 예상되는 불리한 결과의 설명과 해당 업체가 취한 조치의 설명이 포함되어야 한다(제4문). 당사자에게 통지하는 것이 지나치게 비용을 요구하는 경우에는, 특히 관련되는 사안의 수가 너무 많을 때에는 적어도 두 개의 주에 걸쳐서 발행되는 일간신문에 적어도 반 페이지에 달하는 광고를 통해서 또는 관련자의 관점에서 동일한 효력이 있는 적절한 다른 조치를 통해서 정보공시로 대신한다(제5문). 통지의무자의 통지는 자신에 대해서 또는 형사소송법 제52조 제1항에서 규정한 통지의무자의 가족에 대한 형사절차나 질서위반행위법상의 절차에서 통지의무자의 동의하에서만 이용될 수 있다(제6문).

6) 연방정보보호위원회 위원장인 Peter Schaar는 2011년 8월 31일 이 규정의 2년간 시행을 평가하면서 이러한 요청을 함(http://www.bfdi.bund.de/DE/Oeffentlichkeitsarbeit/Pressemitteilungen/2011/30_InformationspflichtBeiDatenpannen.html).

7) Entschließung der 76. Konferenz am 6./ 7. November 2008 Mehr Transparenz durch Informationspflichten bei Datenschutzpannen(http://www.bfdi.bund.de/SharedDocs/Publikationen/Entschliessungssammlung/DSBundLaender/76DSK_Informationspflicht.html?nn=408908).

의무를 준용하고 있는 전기통신법 제93조와 텔레미디어법 제15a조는 공공기관에도 적용된다.[8] 이들 규정은 공공기관과 비공공기관 사이에 구별을 두고 있지 않기 때문이다. 이들 규정은 모든 서비스 제공자들에게 동일하게 적용된다.[9]

2) 업무위탁에 의한 개인정보처리자의 통지의무

업무위탁에 의한 개인정보처리자 본인은 본 규정의 직접적인 수범자는 아니다. 연방정보보호법 제11조 제4항에 의하면 수탁자에 대해서는 연방정보보호법의 특정한 규정에 의해서만 적용된다. 제11조 제4항에는 제42a조가 언급되어 있지 않기 때문에 수탁자에 대해서는 적용되지 않는다. 수탁자에게 위탁에 의하여 저장되어 있는 데이터를 분실한 경우 위탁자가 책임을 진다. 위탁자가 감독기관과 당사자에게 통지하여야 한다. 이를 지체한 경우, 예를 들어 수탁자가 위탁자에게 데이터의 분실을 너무 늦게 알린 경우, 이는 위탁자의 책임으로 된다. 따라서 위탁자는 수탁자가 위탁자에게 지체 없이 신고의무를 부담하도록 하여야 한다. 위탁자는 업무위탁에 의한 개인정보처리 계약에서 명확한 계약상의 의무(연방정보보호법 제11조 제2항 제8호)와 신고절차의 통제를 통해서 이를 달성해야 한다.[10]

3) 통지대상 개인정보

제42a조의 통지의무는 모든 데이터의 유출 및 개인 정보를 대상으로 하는 것이 아니라 특정한 개인정보만을 대상으로 한다. 여기에는 4가지의 범주가 있다. ① 특별한 종류의 개인정보(연방개인정보보호법 제3조 제9항), ② 직업상 비밀에 해당하는 개인정보, ③ 가벌적 행위나 질서위반행위 또는 이와 관련한 혐의를 가지는 개인정보, ④ 은행 및 신용카드회사의 개인정보이다.

(1) 특별한 종류의 개인정보

특별한 종류의 개인정보로는 인종적 · 민족적 출신, 정치적 성향, 종교적 · 철학적 신념, 노동조합가입여부, 건강 및 성생활에 관한 정보 등이다. 특별히 중요한 것은 의료 데이터의 처리 분야(의원, 병원, 보험회사 등)에 있어서 제42a조에 의한 통지의무이다. 또한 누군가가 치료를 받았다는 사실도 건강에 관한 정보가 되기 때문에, 환자의 접촉 데이터도 제42a조 제1항 제1호에 해당될 수 있다.

8) Hornung, Informationen über "Datenpannen" - Neue Pflichten für datenverarbeitende Unternehmen, NJW 2010, p. 1842.

9) Gabel, Voraussetzung für die Informationspflicht TMG §15a, Kommentar zum BDSG und zu den Datenschutzvorschriften des TKG und TMG, p. 1011.

10) FAQs zur Informationspflicht bei unrechtmäßiger kenntniserlangung von Daten nach §42a Bundesdatenschutzgesetz(BDSG)(http://www.datenschutz.rlp.de/downloads/oh/bln_oh_merkblatt_datenpannen.pdf), p. 2.

또한 특별한 개인정보는 인사기록카드가 분실된 경우에도 관계될 수 있다. 진단서 발급이나 병가일수 등이 인사기록카드에 기재되어 있는 경우 이들 데이터도 건강에 관한 정보에 해당한다. 근로소득세의 근거 서류도 종교적 소속에 관한 간접자료가 될 수 있다.

(2) 업무상 비밀에 해당하는 개인정보

업무상 비밀은 비밀준수의 법적 의무이다. 직업상 비밀은 특정한 직업 보유자, 예를 들어 비밀준수자와의 특별한 신뢰관계를 근거로 한 비밀준수자이다. 업무상 비밀준수자는 자기에게 위탁된 정보를 일반적으로 당사자가 동의한 경우에만 공개할 수 있다. 그러한 비밀의 내용에 있어서 개인정보가 문제되고 이것을 권한 없는 제3자가 인식한 경우에는 제42a조가 고려된다.

업무상 비밀에 해당하는 직업그룹은 형법 제203조(사생활의 비밀 침해)에 규정되어 있다. 예를 들어 변호사, 공증인, 의사 등이 여기에 해당한다. 연방정보보호법 제5조에 의한 데이터의 비밀[11]은 직업상 비밀에 해당하지 않는다. 하지만 세무사나 공인회계사는 여기에 해당한다.

민간의료보험, 상해보험, 생명보험회사의 직원들도 경우에 따라서는 업무상 비밀준수자에 해당할 수 있다. 생명보험계약을 체결하였다는 사실은 보험가입자의 직업비밀이 파악되기 때문에 개인정보에 해당한다. 생명보험사와의 계약관계에서 고객과의 접촉 데이터가 분실된 경우에도 제42a조 제1항 제2호와 관련이 있다.

(3) 가벌적 행위나 질서위반행위에 관한 정보

가벌적 행위나 질서위반행위와 관련되는 개인정보에는 형벌구성요건 내지는 질서위반행위의 구성요건과 관련되는 모든 정보가 해당된다. 하지만 적어도 절차가 진행 중이거나 종료된 경우의 정보여야 한다.

그 밖에 제42a조 제1문 제3호는 가벌적 행위나 질서위반행위의 혐의와 관련되는 개인정보가 분실된 경우도 고려된다. 제32조 제1항에 따르면 사업주는 특정한 조건하에서 근로자의 개인정보를 범죄의 적발을 위하여 수집하고, 처리하고 이용할 권리가 있다. 이러한 데이터의 분실의 경우 제42a조에 의한 통지의무가 발생할 수 있다.

(4) 은행 및 신용카드회사의 개인 정보

은행 및 신용카드회사의 개인정보는 계좌와 관련한 전체 정보를 말한다. 신용카드 소유자와 은행계좌 소유자의 성명이 있는 카드번호와 계좌번호가 이에 해당한다. 송금 관련 데이터, 신용카드영수증, 입출금상황 등도 제42a조 제1문 제4호에 해당한다.[12]

11) 연방정보보호법 제5조: 데이터의 처리에 관여한 자는 개인정보를 권한 없이 수집, 처리, 이용해서는 아니된다(데이터 비밀).

12) FAQs zur Informationspflicht bei unrechtmäßiger kenntniserlangung von Daten nach §42a Bundesdatenschutzgesetz(BDSG), p. 5.

4) 통지의무를 부담하게 되는 상황

4가지 범주의 개인정보가 제3자에게 부당하게 전달되거나 그 밖의 다른 방법으로 부당하게 인지된 경우 그리하여 당사자의 권리나 보호될 이익에 대하여 중대한 침해가 위협되는 경우에는 통지의무가 존재한다.

'부당한(unrechtmäßig)'이란 법적 근거 없이 발생하는 경우를 말한다. 당사자가 동의를 하지 않거나 공개가 법률이나 그 밖의 법률 규정에 의해서 허용되지 않는 경우이다.

제3자를 통한 인지는 적극적으로 확인되어야 하는 것은 아니다. 제3자에게 인식되었다는 것이 명료하거나 어느 정도의 개연성을 가진 사실상의 근거에 의해서 이들이 도출되는 경우에는 그것으로 충분하다.

부당한 전달 내지 부당한 인지는 정당하지 않게 수취인을 수집한 경우 또는 데이터가 잘못된 주소로 전달된 경우에 있게 된다. 인터넷에 공개되는 경우도 이에 해당한다. 예를 들어 기술적인 하자로 검색엔진을 통해서 결과가 나타나거나 그 밖의 다른 방법으로 제3자가 접근할 수 있도록 한 경우이다.

통지의무는 또한 데이터를 분실한 경우에도 고려된다. 예를 들어 랩탑이나 다른 저장매체를 제3자가 접근할 수 있는 곳에서 분실하였고 데이터가 암호화되어 있지 않는 경우이다. 데이터를 도둑맞았거나 불법으로 IT 시스템에서 호출될 수 있는 경우에도 있게 된다. 또한 도둑맞은 랩탑의 하드드라이브가 암호화되어 있지 않는 경우에도 인지된 것으로 해석되어야 한다.[13]

5) 중대한 침해의 우려

당사자의 권리나 보호가치가 있는 이익에 대해서 중대한 침해가 우려되는 경우에는 통지의무가 존재한다. 이 경우 제3자를 통한 부당한 인지가 관련 당사자에게 어떠한 영향을 주는지가 중요하다.

책임기관은 진단결정을 해야 한다. 즉 책임기관은 유출사고의 상황에 따른 가능한 결과를 확인하여야 하고 이를 당사자의 부담의 관점에서 그리고 부담이 발생할 개연성의 관점에서 어떠한 잠재적 침해가 실질적 또는 탈비실질적(예를 들어 재산적 손해, 사회적 손실)으로 발생할 수 있는지를 평가하여야 한다. 그런 관점에서 당사자의 권리나 이익이 침해될 가능성이 크면 클수록 개입의 개연성에 관한 요청은 더 적어진다.[14]

6) 통지의 대상

당사자와 관할 감독기관은 제42a조 제1문에

13) FAQs zur Informationspflicht bei unrechtmäßiger kenntniserlangung von Daten nach §42a Bundesdatenschutzgesetz(BDSG), p. 5.

14) Gabel, Voraussetzung für die Informationspflicht TMG §15a, Kommentar zum BDSG und zu den Datenschutzvorschriften des TKG und TMG, p. 1012.

의해서 기본적으로 지체 없이 통지되어야 한다. 감독기관의 통지의 경우에는 책임기관에게 사실관계의 조사와 제42a조의 요건의 심사를 위해서 적합한 기간이 정해져 있다. 이 경우 사고의 복잡성이 중요하다. 기간은 책임기관이 데이터가 전달되거나 부당하게 인식된 사실을 인지한 때부터 시작한다. 감독기관에의 통지에 있어서 모든 보안상의 흠결이 이미 해결되었다거나 형사소추기관의 수사절차가 아직 진행 중이거나 하는 것은 중요하지 않다. 중요한 것은 오로지 제42a조의 사례가 존재하는가이다.

당사자에게 하는 통지는 데이터의 보안을 위한 적절한 조치가 취해지거나 지체 없이 취해지지 않았고, 형사소추가 더 이상 위태롭지 않게 되는 즉시 지체 없이 통지되어야 한다.

책임기관은 감독기관에 대해서 의심이 있는 경우 왜 당사자에게의 통지의 보류가 정당화되었는지를 증명할 수 있어야 한다.

(1) 데이터의 안전성을 위한 적절한 조치

데이터의 안전성을 위한 적절한 조치를 취하는 것이 가능하다면, 당사자에게의 통지는 조치의 성공을 위태롭게 할 우려가 있는 한 유보할 수 있다. 조치가 위해진 즉시 당사자에게 지체 없이 통지하여야 한다. 어떠한 안전적 조치가 고려되는가는 개별적 사례에 달려 있다.

(2) 형사소추의 위태화

형사소추기관의 수사가 위태로울 수도 있는 경우 당사자에게의 통지는 일단 유보된다. 형사소추가 더 이상 위태롭지 않는 경우에 지체 없이 통지되어야 한다. 책임기관은 수사가 공개를 통해서 침해될 수 있는지를 스스로 판단해서는 안 된다. 따라서 형사소추기관, 특히 검찰의 조언을 받는 것이 추천된다.[15]

7) 제공할 정보의 내용

감독기관과 당사자는 부당한 인지의 방법에 대해서 통지를 받아야 한다. 이와 관련하여 구체적으로 정보유출, 즉 직원이나 외부 근무자에 의한 의무위반이나 데이터저장매체의 분실 등이 알려져야 한다. 이 외에 당사자가 불리한 결과를 어떻게 최소화할 수 있는지, 예를 들어 로그인 데이터나 패스워드의 변경 등의 추천이 권고되어야 한다. 감독기관은 또한 가능한 불리한 결과와 그 사이에 취한 조치를 통지받아야 한다.

(1) 감독기관에의 통지

감독기관의 통지는 증명의 근거로 사용하기 위해서 서면으로 하거나 적어도 사후에 보충되어야 한다. 감독기관의 통지에는 다음과 같은 내용이 포함되어야 한다. 즉 ① 데이터가 유출된 일

15) Gabel, Voraussetzung für die Informationspflicht TMG §15a, Kommentar zum BDSG und zu den Datenschutzvorschriften des TKG und TMG, p. 1013.

시, 책임기관이 이를 확인한 때, ② 어떤 데이터가 관련되고 어떻게 이들이 부당하게 전달되었으며 어떻게 부당하게 인지되었는지 그리고 유출사고의 상세한 기록, ③ 부당한 인지로 어떠한 불리한 결과가 가능한지, ④ 책임기관이 취한 조치, ⑤ 당사자에게 이미 통지되었는지 그리고 무엇이 추천되었는지 등이다.

(2) 당사자에게의 통지

당사자에게 부당한 인지의 종류가 설명되어야 하고, 가능한 불리한 결과를 최소화하기 위한 조치가 추천되어야 한다. 이 경우 무엇이 발생하였고, 어떠한 위험이 우려되는지를 당사자에게 투명하고 이해할 수 있게 하는 것이 중요하다. 당사자에게 남용의 위험이 현존해야 한다. 경우에 따라서 이 통지를 통해서 당사자가 예방조치 및 손해방지조치를 취할 수 있도록 되어야 한다. 통지의 내용을 통하여 당사자는 어떠한 위법한 데이터의 이용이 위협될 수 있는지 그리고 이에 대해서 무엇으로 대처할 수 있는지를 예상할 수 있어야 한다. 이를 위해서 또한 당사자는 어떠한 구체적인 데이터가 관련되는지를 알아야 한다. 손해를 최소화하기 위한 조치의 경우에는 구체적인 행위가 추천되어야 한다(예를 들어 신용카드의 교체, 패스워드, 계좌번호나 고객번호의 변경 등). 그 밖의 핫라인 같은 지원서비스도 제공될 수 있다.[16]

8) 통지의 방식

당사자는 기본적으로 개별적으로 통지되어야 한다. 개별적 통지에 대해서는 법률은 특별한 형식을 규정하고 있지 않다. 책임기관은 의심사례에 대하여 증명을 해야 하기 때문에, 당사자에게 통지를 했다는 것을 암호화된 전자우편이나 우편으로 긴급하게 제공되어야 한다. 간단한 편지로 충분한지 등기가 추천되는지는 개별적인 사안에 따라 다르다. 가령 손해배상절차에서는 서신의 도달이 증명될 수 있는 것이 중요하다.

당사자에게의 통지가 비례성을 벗어나는 비용을 요구하는 경우에는 공개정보로 개별적인 통지를 대신한다.

9) 통지의무자의 책임

기업이 개인정보를 유출하게 되는 경우 진퇴양난에 빠지게 된다. 기업이 자신의 정보제공의무를 준수하지 않거나 충분히 하지 않게 되면 제43조[17]의 과태료 구성요건을 충족하게 되지만, 이에 반하여 의무를 수행하게 되면 형사책임이

16) Gabel, Voraussetzung für die Informationspflicht TMG §15a, Kommentar zum BDSG und zu den Datenschutzvorschriften des TKG und TMG, p.1014-1015; FAQs zur Informationspflicht bei unrechtmäßiger kenntniserlangung von Daten nach §42a Bundesdatenschutzgesetz(BDSG), p. 9.

17) 연방정보보호법 제43조 제2항 및 제 3항(범칙금) 제43조 제2항: 제42a조 제1문에 위반하여 고의 또는 과실로 통지를 하지 않거나 정당하게 하지 않거나 완전히 하지 않거나 적시에 하지 않는 자는 질서위반행위를 한 것이다. 제43조 제3항 : 제2항에 의한 질서위반행위는 최고 30만 유로의 과태료가 부과될 수 있다.

나 민사책임의 근거를 형성할 수 있는 상황이 기록으로 남기 때문이다.

(1) 형사책임

형사소추와 관련하여 제42a조 제6항은 형사절차나 질서위반절차에서 증거사용금지를 규정하고 있다. 통지는 단지 통지의무자의 동의에 의해서만 사용될 수 있다. 따라서 형사처벌의 관점에서 신속하고 포괄적인 정보가 제공될 수 있다. 왜냐하면 형사소추를 모면할 기회가 있기 때문이다.

감독기관이나 당사자에게 과실 또는 고의로 통지를 하지 않거나, 정확하게 하지 않거나, 불완전하게 하거나, 적시에 하지 않는 경우에는, 감독기관은 과태료 절차를 제기하여 최고 30만 유로의 과태료를 부과할 수 있다(제43조 제2항 제7호, 제3항).

또한 대가를 위해서 또는 자신이 부당한 이득을 얻거나 다른 사람에게 이를 얻도록 하거나 다른 사람에게 손해를 가할 의도로 통지를 하지 않거나 정당하게 하지 않거나 완전히 하지 않거나 적시에 하지 않는 자는 2년 이하의 자유형 또는 벌금형에 처하도록 하고 있다(제44조 제1항). 이 행위는 고소에 의해서만 소추되고, 고소권자는 당사자, 책임기관, 연방정보보호위원회, 감독기관이다(제44조 제2항)

(2) 민사책임

이에 반하여 민사상 손해배상청구는 증거사용금지와 관련이 없다. 기업은 당사자에게 제7조에 의해서 손해배상청구를 주장하기 위해서 필요한 증거를 정보로 제공한다. 이 청구는 실질적인 손해의 배상으로 제한하고 있다. 물론 데이터 보호의 침해의 경우에는 항상 일반적인 인격권 및 제3자효로 갖추어지는 일반적 인격권(기본법 제2조)과 관련되어, 비실질적 손해의 보상도 포함하는 민법 제823조 제1항에 의한 손해배상청구도 고려된다. 이 밖에 민법 제823조 제2항도 청구의 근거로서 고려된다.[18]

2. 전기통신법(TKG)

2011년 12월 22일 발효된 전기통신법은 제109a조[19]를 통하여 개인정보보호가 침해된 경우

18) Duisberg/Picot, Rechtsfolgen von Pannen in der Datensicherheit, CR 2009, p. 825.

19) 제109a조(데이터안전성) (1) 공중전기통신서비스를 제공하는 자(공중전기통신사업자)는 개인 관련 데이터(개인정보)의 침해의 경우에 지체 없이 연방망규제청과 연방정보보호위원회에 이를 지체 없이 통지하여야 한다(제1문). 개인정보의 보호의 침해를 통하여 통신가입자나 그 밖의 사람의 권리나 보호이익이 중대하게 침해된다는 것이 예상되는 경우에는 전기통신사업자는 추가로 당사자에게 지체 없이 이러한 침해를 통지하여야 한다(제2문). 침해된 관련 데이터가 적절한 기술적 조치를 통하여 확보되고, 특히 안전한 것으로 인정된 암호화절차의 적용으로 저장되었다는 안전구상(Sicherheitskonzept)이 증명된 경우에는 통지는 필요하지 않다(제3문). 제3문과 무관하게 연방망규제청은 있을 법한 개인정보보호의 침해의 불리한 효과를 고려하여 당사자에게의 통지를 하게 할 의무를 통신사업자에게 부과할 수 있다(제4문). 그 밖의 경우에 대해서는 연방정보보호법 제42a조 제6문을 준용한다(제5문). 통지의무자가 행하는 통지는 자신에 대해서 또는 형사소송법 제52조 제1항에서 규정한 통지의무자의 가족(구성원)에 대한 형사절차나 질서위반행위법상의 절차에서 단지

에 연방방망규제청, 연방정보보호위원회(BfDI), 특정한 상황에서 당사자에게 대해서도 통지의무를 규정하고 있다.[20]

1) 통지의무자

의무자는 제109a조에 의한 공중통신망서비스를 제공하는 자이다(전기통신사업자). 물적 적용범위는 개인정보보호의 침해로 규정되어 있다. 전기통신법 제3조 제30a호에는 이 개념을 법적으로 정의하고 있다. 이에 의하면 '개인정보보호의 침해'란 개인정보의 안전성의 침해와 이에 대한 부당한 접근이다. 개인정보가 전달되거나 저장되거나 그 밖의 방법으로 공중통신서비스의 제공과 함께 처리되어야 하는데, 이것이 유출(분실), 부당한 삭제, 변경, 저장, 전달 및 그 밖의 부당한 이용으로 되어야 한다. 따라서 적용범위는 이용자 기본정보와 통신정보에 한정되지 않는다.

2) 통지의무

전기통신사업자는 2단계의 통지의무를 부담한다. 1단계는 일반적인 개인정보보호가 침해되는 경우를 규정하고 있다. 즉 전기통신사업자는 개인정보보호가 침해되는 모든 경우에 지체없이 연방망규제청과 연방정보보호청에 통지하여야 한다(전기통신법 제109a조 제1항 제1문). 2단계는 중대한 침해가 있는 경우 당사자에게 해야 하는 통지의무를 규정하고 있다. 개인정보보호의 침해로 통신가입자나 그 밖의 사람의 권리나 보호이익이 중대하게 침해된다는 것이 예상되는 경우에는 전기통신사업자는 당사자에게도 지체 없이 이러한 침해를 통지하여야 한다(전기통신법 제109a조 제1항 제2문).

하지만 통지의무의 예외가 있다. 즉 안전성구상(Sicherheitskonzept)을 통하여 적절한 기술적 조치가 당해 데이터의 확보를 위해서 증명된 경우 당사자에게의 통지는 유보될 수 있다. 이러한 적절한 기술적 조치가 무엇인지는 연방망규제청에 의해서 작성된다. 연방망규제청은 연방정보기술안전청과 연방정보보호위원회의 동의로 전기통신시스템과 데이터처리시스템의 운영과 적절한 기술적 조치 및 그 밖의 조치를 위한 안전 요구사항의 목록을 작성하여야 하는데(전

통지의무자의 동의하에서만 이용될 수 있다(제6문). (2) 당사자에게 하는 통지에는 적어도 다음의 내용이 포함되어야 한다. 1. 개인정보 보호의 침해의 종류, 2. 그 밖의 정보를 획득할 수 있는 연락처에 관한 정보, 3. 개인정보보호의 침해로 예상되는 사후 부작용을 제한하는 조치의 추천. 연방망규제청과 연방정보보호위원회에 해야 하는 통지에는 추가로 개인정보보호의 침해의 결과와 의도하였거나 취해진 조치가 설명되어야 한다. (3) 통신사업자는 개인정보 보호의 침해 목록을 작성해야 한다. 다음의 정보가 포함되어야 한다. 1. 피해 상황, 2. 피해의 영향, 3. 행해진 구제조치. 이러한 정보들은 연방망규제청과 연방정보보호위원회가 제1항과 제2항의 규정들이 준수되었는지를 심사할 수 있도록 하기 위해서 충분해야 한다. 이 목록은 이러한 목적에 필요한 정보만을 포함해야 하고 5년이 지난 침해는 고려되어서는 안된다. (4) 유럽연합지침 2002/58/EG 제4조 제5항에 의한 유럽연합집행위원회의 기술적 이행조치를 조건으로 하여 연방망규제청은 형식, 절차의 방식, 개인정보보호의 침해에 통지가 필요한 상황과 관련하여 지침을 규정할 수 있다.

20) Entwurf eines Gesetzes zur Änderung telekommunikationsrechtlicher Regelungen, BT-Drucksache 17/5707, 04.05.2011, p. 33, p.83~84(http://dipbt.bundestag.de/dip21/btd/17/057/1705707.pdf).

기통신법 제109조 제6항), 여기에 적절한 기술적 조치를 포함시킬 수 있기 때문이다.

3) 통지의 내용

전기통신사업자가 우선 당사자 및 연방망규제청과 연방정보보호위원회에게 공통으로 통지해야 하는 내용은 ① 개인정보 보호의 침해의 종류, ② 그 밖의 정보를 획득할 수 있는 연락처에 관한 정보, ③ 개인정보보호의 침해의 가능한 사후 부작용을 제한하는 조치의 추천이다. 전기통신사업자는 별도로 연방망규제청과 연방정보보호청에게 개인정보보호의 침해의 결과와 의도한 조치 및 취해진 조치가 설명되어야 한다(제109a조 제2항).

4) 개인정보의 보호침해에 관한 목록

전기통신사업자는 그 밖에 개인정보의 보호의 침해의 목록을 작성해야 하는데, 여기에는 피해 상황, 피해의 영향, 행해진 구제조치가 포함되어야 한다. 이러한 정보들은 연방망규제청과 연방정보보호위원회가 제1항과 제2항의 규정들이 준수되는지를 통제할 수 있도록 해야 한다(제109a조 제3항).

5) 통지의 개별성에 관한 지침

연방망규제청은 필요한 경우 통지의 구체적인 내용과 관련하여 지침을 제정할 수 있다. 이 지침은 특히 형식, 절차, 개인정보보호의 침해에 관한 통지가 요청되는 상황 등이 들어 있어야 한다(제109a조 제4항).

3. 텔레미디어법(TMG)

1) 제15a조 – 데이터의 부당한 인식획득의 경우 통지의무

서비스제공자의 통지의무는 자신에게 저장된 이용자기본정보(Bestandsdaten)나 이용정보(Nutzungsdaten)가 부당하게 제3자에게 전달되거나 그 밖의 방법으로 제3자에게 부당하게 인지되어, 해당 이용자의 권리나 보호이익이 중대하게 침해될 우려가 있는 것이 확인된 경우에 존재한다.

텔레미디어법 제15a조는 연방정보보호법 제42a조의 적용범위를 영역에 특별하게 텔레미디어법 제14조, 제15조에 의한 이용자기본정보와 이용정보에도 확대한 것이다. 따라서 이 규정은 특별규정이고 법적 효과에 해당하는 연방정보보호법 제42a조를 준용을 포함하고 있다. 게다가 제15a조는 제13조 제1항, 제3항, 제5항, 제6항, 제15조 제3항에 의한 데이터보호법상의 통지의무를 보충하고 있다. 텔레미디어법상의 특수성을 중심으로 설명한다.

2) 요건

(1) 서비스제공자(Diensteanbieter, ISP)

통지의무자는 서비스제공자이다. 서비스제공

자는 텔레미디어법 제2조 제1호에 법적 개념이 규정되어 있다. 이에 따르면 서비스제공자는 자신 또는 타인의 텔레미디어를 이용에 제공하거나 이용을 위한 접근을 중개하는 자연인 또는 법인으로 규정되어 있다. 서비스제공자의 개념에는 공법상의 단체나 그 밖에 법적 능력 있는 공법상의 시설(가령 종합대학이나 전문대학)도 해당한다. 이것은 텔레미디어법 제1조 제1항 제2문에서 나온다. 이에 의하면 이 법률은 공공기관을 포함한 모든 제공자에게 적용된다고 하고 있기 때문이다. 따라서 연방뿐만 아니라 각 주도 텔레미디어법의 데이터보호규정이 적용된다. 이러한 면에서 텔레미디어법 제15a조에 의한 통지의무자의 적용범위는 연방정보보호법 제42a조에 의한 적용범위보다 넓다. 연방정보보호법 제27조 제1항 제1문 제2호에 언급된 공법상의 사업체만을 그 적용범위로 하고 있기 때문이다.[21]

(2) 이용자기본정보 및 이용정보

통지대상 정보는 서비스제공자에게 저장되어 있는 이용자기본정보 및 이용정보이다. 이들 정보들은 법적 개념으로 제14조 제1항과 제15조 제1항 제1문에 각각 규정되어 있다.

이용자기본정보란 텔레미디어의 이용에 관한 서비스제공자와 이용자 사이에 계약관계의 근거, 내용의 형성 또는 변경을 위해서 필요한 경우 서비스제공자가 수집하고 이용하는 이용자의 개인정보를 말한다(제14조 제1항). 이용정보란 텔레미디어의 이용을 가능하게 하고 전산을 위해서 필요한 경우 서비스제공자가 수집하여 이용할 수 있는 이용자의 개인정보를 말한다(제15조 제1항). 이러한 개인정보에는 다음의 개인정보가 포함된다. ① 이용자의 신원확인을 위한 표지, ② 이용의 시작과 종료 및 범위, ③ 이용자가 이용한 텔레미디어에 관한 정보 등.

(3) 중대한 침해

제15a조의 통지의무의 요건은 관련 이용자의 권리나 보호이익에 대한 중대한 침해를 요건으로 한다. 중대한 침해의 개념은 기본적으로 연방정보보호법 제42a조의 개념과 동일하다. 연방정보보호법 제42a조는 통지의무를 야기하는 데이터의 종류를 특별한 민감성에 따라서 구별하고 있는 데 반하여, 텔레미디어법은 그렇지 않다. 가령 이용자의 성명과 주소와 같은 순수한 이용자기본정보는 연방정보보호법 제42a조에서 규정한 데이터의 종류보다는 민감성에서 상당히 떨어진다. 따라서 텔레미디어법 제15a조의 적용범위에 있어서 해당 데이터의 종류와 관련하여 상당한 재량이 존재할 수 있다.[22]

(4) 법적 효과

제15a조의 법적 효과는 연방정보보호법 제42a조를 준용하고 있다. 따라서 해당 요건들이 존재

21) Moos, TMG §15a, Kommentar zum BDSG und zu den Datenschutzvorschriften des TKG und TMG, p. 1140.
22) Moos, TMG §15a, Kommentar zum BDSG und zu den Datenschutzvorschriften des TKG und TMG, pp. 1140~1141.

하는 경우 서비스제공자는 데이터의 부당한 인지를 지체 없이 관할기관과 관련 당사자들에게 통지해야 한다.

제42a조와는 달리 제15a조에서는 통지의무의 침해에 대해서 과태료 규정이 없다. 이는 입법자의 과오로 인정되고 있다. 따라서 질서위반법 제3조에 의한 유추적용금지를 근거로 하여 제15조의 위반에 대한 처벌은 불가능하다.[23]

4. 베를린주 정보보호법(Berliner Datenschutzgesetz)

1) 개관

베를린주는 2011년 2월 2일 베를린주 정보보호법을 개정하였다. 이 개정에서 정보유출의 경우 책임기관의 통지의무를 비공공기관뿐만 아니라 베를린주 내의 모든 공공기관으로 확대하였다. 이러한 확대는 독일에서는 처음 입법이다. 연방과 각주의 정보보호위원들은 2010년 이러한 통지의무를 모든 공공기관으로 확대할 것을 요청한 바 있다. 이 제안을 베를린주 입법자는 수용한 것이다.[24]

2) 제3자에 의한 정보의 부당한 인지의 경우 통지의무

데이터 처리 기관이 자신에게 저장되어 있는 개인정보가 부당하게 제3자에게 전달되고 있거나 그 밖의 다른 방법으로 제3자에게 인지되고 있어서 당사자의 권리나 보호이익이 중대하게 침해될 우려가 있는 것을 알고 있는 경우에는, 지체 없이 이를 당사자나 베를린 정보보호위원에게 통지하여야 한다(제18a조 제1항).

당사자에게의 통지의무는 책임기관이 우선 데이터의 안전을 위하여 적절한 조치를 취한 경우에 유예될 수 있다. 하지만 책임기관이 이 조치를 지체 없이 하지 않는 경우에는 당사자에게의 통지는 유예되지 않는다. 당사자에게의 지체 없는 통지가 형사소추를 위태롭게 할 우려가 있는 경우에도 이러한 통지는 유예되지 않는다. 책임기관은 부당한 인지의 종류와 가능한 불리한 결과를 최소화하기 위한 조치를 당사자에게 통지하여야 한다. 당사자에 대한 통지가 상당한 비용이 지출될 우려가 있는 경우에는 그 대신에 적절한 정보의 공개로 대신할 수 있다.[25]

3) 제재

과태료 부과규정은 연방정보보호법 제43조가 준용된다. 즉 감독기관이나 당사자에게 과실 또는 고의로 통지를 하지 않거나, 정확하게 하지 않거나, 불완전하게 하거나, 적시에 하지 않는 경우에는, 감독기관은 과태료 절차를 제기하여 최고 30만 유로의 과태료를 부과할 수 있다(제43조 제

23) Moos, TMG §15a, Kommentar zum BDSG und zu den Datenschutzvorschriften des TKG und TMG, p. 1141.
24) Dix, Alexander, Berliner Datenschutzgesetz, 2011.5, p. 3.
25) Dix, Alexander, Berliner Datenschutzgesetz, 2011.5, p. 23.

2항 제7호, 제3항).

Ⅳ. 맺음말

독일의 경우 개인정보의 유출과 관련하여 개인정보가 부당하게 제3자에게 전달되거나 인지되어 당사자의 권리나 보호이익이 중대하게 침해될 우려가 있는 경우에 관할 감독기관과 당사자에 통지하는 제도를 두고 있다. 우선 정보가 유출된 경우 책임기관은 조치를 취하여야 하고 감독기관이나 당사자에게 통지를 하여야 한다. 이러한 통지를 제대로 하지 않을 경우 과태료나 형사처벌을 받게 된다. 이러한 면에서 독일의 법제는 개인정보의 유출 자체에 대한 직접적인 규제라기보다는 간접적인 규제라고 할 수 있다.

박 희 영

(해외입법조사위원,

독일 막스플랑크 국제형법연구소 연구원)

참고문헌

문헌

Duisberg/Picot, Rechtsfolgen von Pannen in der Datensicherheit, CR 2009, p. 825.

Hornung, Informationen über "Datenpannen" - Neue Pflichten für datenverarbeitende Unternehmen, NJW 2010, p. 1842.

Karger, Michael, Informationspflichten bei Data Breach § 42a BDSG: Handhabung in der Praxis, ITRB 7/2010.

Moos, Flemming, TMG §15a, Kommentar zum BDSG und zu den Datenschutzvorschriften des TKG und TMG, p. 1140.

웹사이트

30. Tätigkeitsberichte des LfD Baden-Würtenberg, p. 23.

Entschließung der 76. Konferenz am 6./ 7. November 2008 Mehr Transparenz durch Informationspflichten bei Datenschutzpannen(http://www.bfdi.bund.de/SharedDocs/Publikationen/Entschliessungssammlung/DSBundLaender/76DSK_Informationspflicht.html?nn=408908).

Entwurf eines Gesetzes zur Änderung telekommunikationsrechtlicher Regelungen, BT-Drucksache 17/5707, 04.05.2011, p. 33, pp. 83~84.

FAQs zur Informationspflicht bei unrechtmäßiger kenntniserlangung von Daten nach §42a Bundesdatenschutzgesetz(BDSG)(http://www.datenschutz.rlp.de/downloads/oh/bln_oh_merkblatt_datenpannen.pdf).

Ponemon Institute, 2010 Annual Study : German Cost of a Data Breach, p.12(http://www.symantec.com/content/de/de/about/downloads/press/2010_annual_study.pdf).

http://www.bfdi.bund.de/DE/Oeffentlichkeitsarbeit/Pressemitteilungen/2011/30_InformationspflichtBeiDatenpannen.html.

http://www.bfdi.bund.de/DE/Oeffentlichkeitsarbeit/Pressemitteilungen/2011/30_InformationspflichtBeiDatenpannen.html.