

PRIVACY BY TRUST, TRUST BY PRIVACY

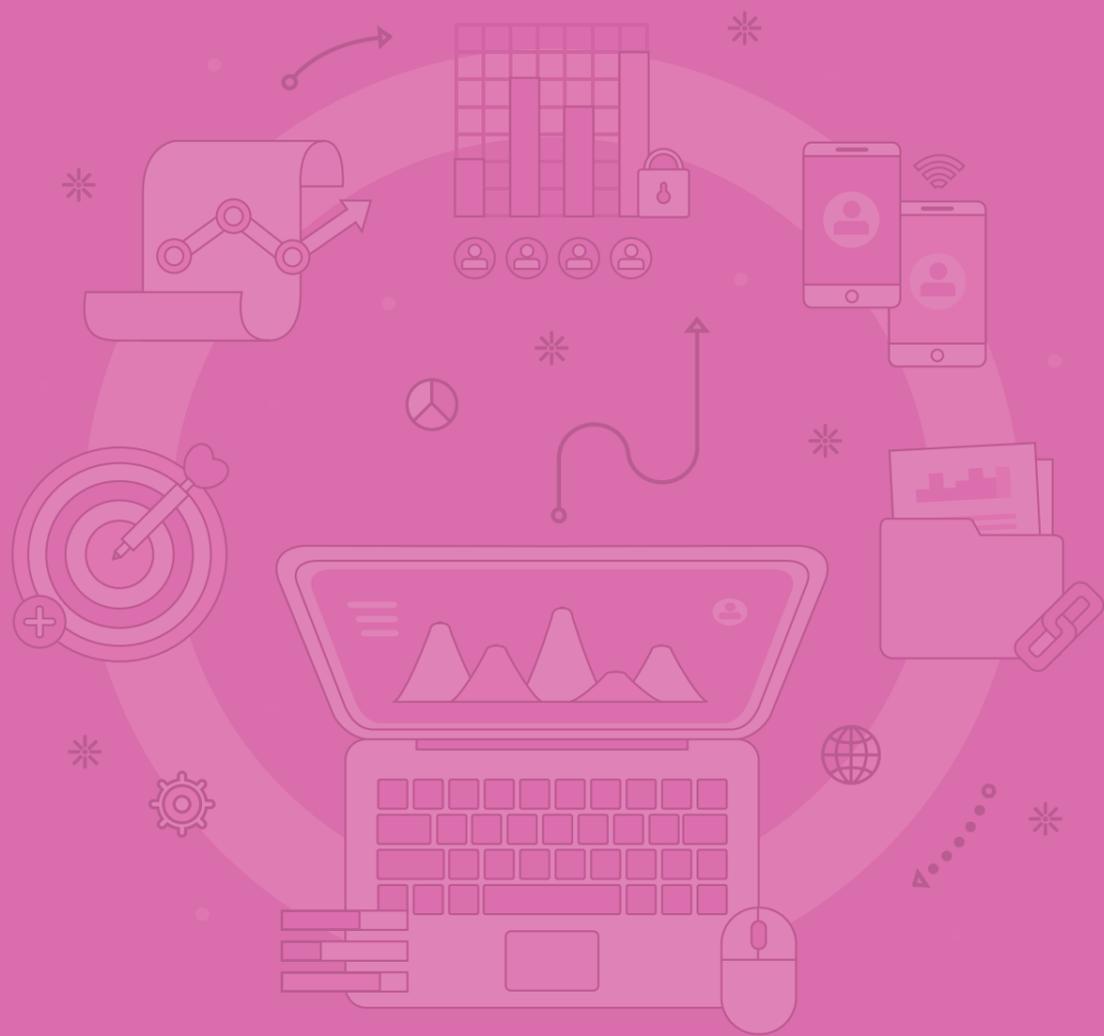
글로벌 개인정보보호 규제 체계 현황 조사

2021





독일



I. 법률체계

1. 개요

은 2018년 5월 25일부터 시행된 EU의 일반 개인정보 보호법(GDPR, General Data Protection Regulation)을 근간으로 연방과 주에서 각각 개인정보 보호법을 개정하여 시행하고 있다. 새롭게 전면 개정된 연방 개인정보 보호법(BDSG, Neue Bundesdatenschutzgesetz)의 경우, GDPR의 시행에 맞춰 EU 회원국 각자가 자국 내 상황에 맞게 규정을 수정해 반영할 수 있는 개별 위임 조항(Opening Clauses)을 구체화 하고, 기존의 법제를 GDPR에 맞추어 2018년 5월 25일부터 시행하고 있다. 주별 개인정보 보호법도 GDPR과 새로운 연방 개인정보 보호법에 따라 개정이 이루어지고 있다.

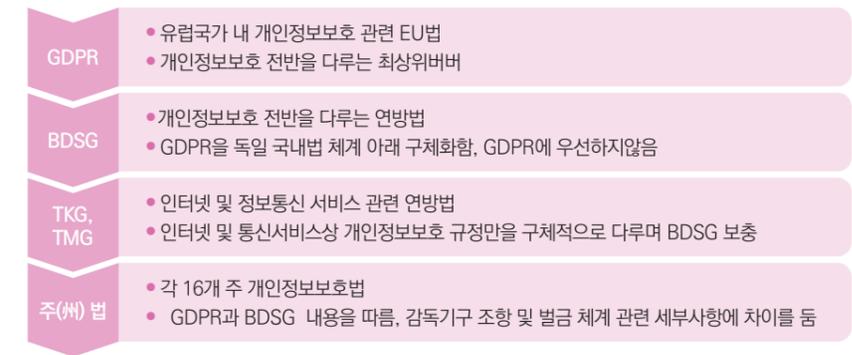
2. 법률 체계

가. 개요

GDPR은 EU 회원국이 준수해야 할 법으로, GDPR이 직접 적용되는 범위에 독일 연방 개인정보보호법(BDSG)은 적용되지 않는다 (BDSG 제1조제5항). 다만 GDPR에는 약 70개의 개별 위임 조항이 있는데, 이들 조항은 각 회원국의 특색에 맞도록 조정할 수 있는 부분적인 선택 사항을 담고 있다. 따라서, BDSG는 GDPR이 개별 회원국 법률에 위임한 범위 내(예: 당국 및 공공 기관에 의한 개인정보 처리, 고용 관계에서의 비디오 감시 및 개인정보 처리 등)에서 적용되나, 만약 개별 주(州)의 개인정보보호법에서 별도의 정한 바가 있다면, 주(州) 개인정보보호법 조항이 BDSG 보다 우선 적용되는 법체계적 특색을 나타낸다.

각 주 개인정보보호법은 GDPR과 BDSG의 주요 골자를 따르며 GDPR과 BDSG에 확정되지 않은 세부사항을 보완한다. 위의 일반 개인정보 보호법 이외에 연방 법률인 통신 및 텔레미디어 개인정보 보호법(Telekommunikation-Telemedien-Datenschutz-Gesetz, TTDSG)은 기존 정보통신법(TMG)과 텔레커뮤니케이션법(TKG)의 개인정보 보호 조항을 대체하여 인터넷, 정보통신 및 텔레미디어의 개인정보보호를 구체적으로 다룬다. 해당 연방법은 GDPR과 BDSG를 보완한다.

[그림 1] 독일 개인정보보호법 체계



나. 특별법

BDSG와 주 개인정보보호법을 제외하고 개인정보보호 관련 규정들이 다른 특별법에 분산되어 있다. 이는 EU차원 GDPR 개인정보보호법이 구체화되기 이전 개인정보보호 관련 독일 국내법을 추가적으로 보완한 결과이다. 개인정보보호 관련 내용을 포함한 법으로는 통신 및 텔레미디어 개인정보 보호법(TTDSG), 돈세탁방지법(Geldwäschegesetz), 에너지경제법(Energiewirtschaftsgesetz)이 있다. 이중 TTDSG는 온라인 개인정보 보호 및 보안을 규정하는 법률이기에 온라인 서비스 사업체는 해당 법률을 숙지할 필요가 있다.

다. 주별 개인정보 보호법

독일의 개인정보보호법은 공공과 민간을 모두 규율하는 일반법 차원의 연방 개인정보보호법이 있고, 베를린 등과 같이 주별 개인정보 보호법이 있다.

[표 1] 주별 개인정보 보호법

주(land)	개인정보 보호법 링크
바덴-뷔르템베르크 (Baden-Württemberg)	https://www.baden-wuerttemberg.datenschutz.de/wp-content/uploads/2018/06/LDSG-neu-GBI-2018173.pdf
바이에른(Bayern)	http://gesetze-bayern.de/Content/Document/BayDSG?AspxAutoDetectCookieSupport=1 https://www.datenschutz-bayern.de/datenschutzreform2018/
베를린(Berlin)	https://www.datenschutz-berlin.de/berliner-datenschutzrecht.html
브란덴부르크 (Brandenburg)	https://dsgvo-gesetz.de/bbgdsg/
브레멘(Bremen)	https://www.datenschutz.bremen.de/rechtsgrundlagen/landesebene-11547

함부르크(Hamburg)	https://datenschutz-hamburg.de/pages/hmbdsg/
헤센(Hessen)	https://datenschutz.hessen.de/infothek/gesetze
메클렌부르크-포어포머른 (Mecklenburg-Vorpommern)	https://www.datenschutz-mv.de/datenschutz/rechtsgrundlagen/
니더작센(Niedersachsen)	http://www.lfd.niedersachsen.de/recht/nieders_recht/ndsg/das-niedersaechsische-datenschutzgesetz-56264.html
노트라인-베스트팔렌 (Nordrhein-Westfalen)	https://www.lfd.nrw.de/mainmenu_Gesetze/submenu_Datenschutz/Inhalt/NationalesRecht/index.php
라인란트-팔츠 (Rheinland-Pfalz)	http://landesrecht.rlp.de/jportal/?quelle=jlink&query=DSG+RP&psml=bsrlprod.psm1
자란트(Saarland)	https://dsgvo-gesetz.de/sdsg/
작센(Sachsen)	https://www.revosax.sachsen.de/vorschrift/1672-Saechsisches-Datenschutzgesetz
작센-안할트 (Sachsen-Anhalt)	http://www.landesrecht.sachsen-anhalt.de/jportal/portal/t/or0/page/bssahprod.psm1?pid=Dokumentanzeige&showdoccase=1&js_peid=Trefferliste&documentnumber=1&numberofresults=1&fromdoctodoc=yes&doc.id=jlr-DSGST2015rahmen&doc.part=X&doc.price=0.0
슐레스비히-홀스타인 (Schleswig-Holstein)	https://www.datenschutzzentrum.de/gesetze/
튀링엔(Thüringen)	https://dsgvo-gesetz.de/thuerdsg/

3. 연방 개인정보 보호법(BDSG Neue Bundesdatenschutzgesetz)

가. 개요

독일의 연방 개인정보 보호법은 개인정보 법제에 있어 가장 중심이 되는 법률로서 전체 4부, 19장, 2절, 86조로 구성되어 있다. 제1부는 일반 규정, 제2부는 GDPR의 이행 규정들, 제3부는 'EU 형사사법절차에서 개인정보보호지침'(Directive (EU) 2016/680)의 이행 규정들, 제4부는 GDPR과 'EU 형사사법절차에서 개인정보보호지침'(Directive (EU) 2016/680)이 적용되지 않는 영역에서의 처리를 위한 특별 규정들로 이루어져 있다.

나. 개인정보 및 민감정보 정의

BDSG에는 개인정보 또는 민감정보에 대한 개념을 정의하고 있지 않으므로, 해당 내용은 GDPR 규정을 그대로 따르게 된다. 따라서,

“개인정보”란 식별되었거나 또는 식별 가능한 자연인(정보주체)과 관련된 모든 정보를 의미하며, 특히 이름, 식별 번호,

소재지 데이터, 온라인 식별자, 정신적·경제적·문화적·사회적 고유성에 관한 모든 정보를 뜻한다.

또한 “민감정보”란 인종 또는 민족, 정치적 견해, 종교적·철학적 신념, 노동조합의 가입 여부를 나타내는 개인정보의 처리와 유전자 정보, 개인을 고유하게 식별할 수 있는 생체정보, 건강정보, 성생활 또는 성적 취향에 관한 정보를 의미한다.

다. 적용 범위

BDSG 제1조는 동 법률의 적용범위를 규정하고 있다. 제1조제1항은 BDSG가 연방 공공기관과, 주(州) 개인정보보호법이 적용되지 않는 주 공공기관의 개인정보 처리에 적용된다고 명시하고 있으며, 또한 민간 부문의 경우 전적 또는 부분적으로 자동화 방식에 의해 이루어지는 개인정보의 처리와 자동화 수단 이외의 방식에 의한 것으로서 파일시스템을 구성하거나 구성하기 위한 개인정보의 처리에 적용된다고 규정하고 있다. 다만, 자연인이 순수하게 개인활동 또는 가정활동을 하는 중에 이루어지는 처리에는 적용되지 않는다.

BDSG 제1조제4항에서는 적용대상을 규정하고 있다. 즉, 동 법률은 공공기관에 적용되며, 민간 부문의 경우 ▲독일에서 컨트롤러 또는 프로세서가 개인정보를 처리하거나 ▲컨트롤러 또는 프로세서의 독일 내 사업장의 활동에 수반되는 개인정보 처리이거나 ▲컨트롤러 또는 프로세서가 EU 회원국 내 또는 유럽 경제 지역(European Economic Area) 내 사업장이 없으나 GDPR의 적용범위에 해당될 경우에는 민간 부문도 BDSG의 적용대상이 된다.

라. 개인정보처리 동의

BDSG에서는 ‘동의’에 관해 규정하고 있지 않아 GDPR 규정을 그대로 따른다. GDPR 제4조제11항은 동의를 ‘본인과 관련된 개인정보의 처리에 대해 합의한다는 의사표시로, 정보주체의 희망 진술 또는 명백한 적극적인 행위를 통해 자유롭고, 구체적으로, 결과에 대해 인지하여 분명하게 나타낸 것’이라고 정의하고 있다. 정보주체의 동의는 컨트롤러의 개인정보 처리 적법성의 한 요건에 해당하기도 하는데(GDPR 제6조제1항), 무엇보다도 적극적인 의사표시 행위로서 이루어져야 하므로 침묵이나 웹사이트 상에서 사전 자동체크 된 형식의 동의, 부작위에 의한 동의는 허용되지 않는다 (전문 제32항).

한편, 정보주체는 자신이 의사 표시한 동의를 언제든지 철회할 수 있으며, 동의 철회권에 대해서는 동의를 제공하기 전에 해당 권리를 행사할 수 있음을 고지 받아야 한다. 동의 철회는 동의의 제공만큼 용이하게 행사할 수 있어야 하며, 동의를 철회하더라도 철회 이전에 동의를 기반으로 한 정보 처리의 적법성에는 영향을 미치지 않는다. (제7조제3항)

마. 정보주체의 권리

(1) 정보를 제공받을 권리

BDSG 제32조~제33조는 개인정보수집 및 처리에 관한 정보가 정보주체에 제공되어야 한다고 규정한다. 이는 GDPR 제12조~제14조에 상응하는 내용이며, 정보주체는 컨트롤러로부터 정보수집 목적, 처리권한등을 고지 받을 권리가 있다. 또한 정보주체의 개인정보 처리와 관련해 해당 컨트롤러가 지정한 DPO, 개인정보 감독기구 연락처 역시 정보주체에게 전달되어야 한다. 정보주체가 개인정보에 대해 가지는 권리, 이를테면 감독기구에 민원을 제기할 권리와 개인정보의 국외이전에 관한 요건 역시 알 수 있어야 한다.

(2) 접근권

접근권이란 정보주체 자신의 개인정보 열람 권한을 뜻한다. 정보주체는 수집 및 처리되는 개인정보에 접근할 수 있어야 한다. 또한 수집된 정보의 출처, 처리 목적, 정보 열람자 범위, 정보 소장 기간 등에 대한 내용을 열람할 수 있거나, 자신과 관련된 데이터를 어떻게 처리하고 있는지 여부에 대한 정보를 제공 받을 수 있어야 한다. 컨트롤러는 정확하고 이해하기 쉬우며 쉽게 접근할 수 있는 형식으로 명확하고 간단한 언어를 사용하여 정보주체와 의사소통해야 할 의무가 있다. 따라서 컨트롤러는 정보주체의 열람 요청에 대응해야 하며 정보주체가 열람하는 데 장애를 두어서 안 된다.

접근권은 GDPR 제15조에 근거를 두고 있는데, BDSG는 제34조에서 접근권 행사의 제한 사유를 열거하고 있다. 즉, 개인정보를 보존하도록 규정하고 있는 법령상의 조항이나 단순한 개인정보보호 목적의 모니터링을 이유로 개인정보가 기록되어 있는 경우에, 정보를 제공하는 것이 불균형적인 노력을 요하거나 타 목적을 위한 개인정보 처리를 불가능하게 하는 기술적, 관리적 조치를 요할 경우 정보주체의 접근권이 제한된다. 마찬가지로 공공당국의 판단에 따라, 컨트롤러가 개인정보를 공개하는 것이 연방 또는 주(州)의 공공의 이익에 해가 되는 경우에도 정보주체의 접근권 행사가 제한된다. 이 경우, 컨트롤러는 정보 제공을 거부하는 이유를 문서화해야 하며 그 거부 사유를 정보주체에게 알려야 한다.

(3) 삭제권

BDSG 제35조는 '삭제권'이라는 제목을 두고 있으면서도 정보주체의 삭제권 행사가 제외되는 사유만을 열거하고 있으며, 실질적으로는 컨트롤러의 '처리제한 의무'를 주로 규정하고 있다. 구체적으로, ▲자동화되지 않는 개인정보 처리의 경우에 삭제가 불가능하거나 특별한 저장 유형으로 인해 지나치게 많은 노력을 기울여야만 삭제가 가능하고 삭제에 대한 정보주체의 법익이 낮은 것으로 간주되는 경우 ▲수집된 개인정보가 처리 목적에 더 이상 필요하지 않은 경우와 개인정보가 불법적으로 처리된 경우라 할지라도, 컨트롤러가 개인정보 삭제가 정당한 이익에 부정적인 영향을 미칠 것이라고 판단하는 경우 ▲개인정보 삭제가 법령이나 계약에 반하는 상황에서 수집된 개인정보가 목적에 더 이상 필요하지 않은 경우, 컨트롤러는 삭제 의무 대신 처리제한 의무를 부담하게 된다. 결국 정보주체는, BDSG 제35조에 따라 삭제권이 제한되는 경우 이외에는 GDPR 제17조에 따라 삭제권을 행사할 수 있다.

(4) 반대권

정보주체는 GDPR 제21조에 따라 자신의 개인정보에 대한 처리 및 수집에 원칙적으로 반대할 수 있으나 일부 특수한 경우에는 반대권이 인정되지 않는다. BDSG 제36조는 정보주체의 이익을 초과하여 처리에 긴급한 공공성이 있거나 법에 따라 처리가 필요한 경우 공공기관에 대한 정보주체의 반대권이 보장되지 않는다고 규정하고 있다. 또한, BDSG 제27조에 따라 개인정보가 과학적 또는 역사적 연구 목적과 통계적 목적을 위하여 처리될 때에, 연구 또는 통계 목적 달성이 불가능하거나 심각하게 저해될 가능성이 있으면서 해당 목적의 이행을 위하여 반대권 제한이 필요한 경우에는 해당 범위 내에서 반대권 행사가 제한될 수 있다.

바. 컨트롤러 및 프로세서의 의무

(1) 개요

BDSG는 DPO 지명(제38조) 이외에는 컨트롤러 및 프로세서의 의무에 대해 별도 규정을 두지 않고 있어, 해당 의무사항 역시 GDPR 규정이 그대로 적용된다. 즉, 컨트롤러 및 프로세서는 GDPR 규정에 따라 처리 활동 기록(GDPR 제30조), 개인정보 영향평가(GDPR 제35조)와 관련한 의무를 부담하며, DPO 지정과 관련해서는 BDSG 제38조를 따른다.

(2) 개인정보 처리 활동 기록 의무

GDPR 제30조에 따라 컨트롤러와 프로세서는 개인정보 처리활동 기록을 보존해야 한다. 처리활동 기록에는 컨트롤러와 DPO의 이름 및 연락처, 개인정보 수집 및 처리 목적 등을 명시해야 한다. 또한 정보주체와 수집된 개인정보의 카테고리, 이와 관련한 설명 및 수집 정보의 저장기간과 삭제 예정 기한, 정보처리에 적용되는 기술적, 관리적 조치에 대한 정보도 모두 포함되어야 한다.

처리 활동 기록을 보존해야 할 의무대상은 종업원 수 250명 이상을 보유한 기업을 원칙으로 한다. 단, ▲정보주체의 권리와 자유에 위험을 초래할 가능성이 있는 개인정보를 처리하거나 ▲민감한 개인정보를 처리하거나 ▲범죄경력 및 범죄행위에 관련된 개인정보를 처리하는 기업은 종업원 수에 관계없이 처리활동 기록을 보존해야 한다. (GDPR 제30조제5항)

(3) 개인정보 영향 평가

컨트롤러는 개인정보처리 기술 및 시스템을 도입하기 이전에 해당 기술·시스템이 초래할 위험을 미리 예상 및 진단해야 한다. 즉, 컨트롤러는 개인정보의 처리 형태(신기술 사용 시) 및 유형, 처리 목적 및 범위, 처리 상황 등으로 인해 정보주체의 법익에 상당한 위험을 초래할 가능성이 있는 경우, 처리 이전에 처리 작업이 개인정보 보호에 미치는 영향에 대한 평가를 수행해야 한다. 이 때 침해의 위험성이 높은 유사한 업무 분야의 경우, 한 번의 평가로 중대한 위험을 초래하는 일련의 유사 처리 작업을 다룰 수 있다.

영향평가를 수행할 경우에는 최소한 ▲예정된 처리 업무 및 처리 목적에 대한 체계적인 설명 ▲목적과 관련한 개인정보 처리의 필요성과 비례성에 대한 평가 ▲정보주체의 법익에 대한 위험 평가 ▲정보주체의 권리 보장과 보안에 관한 예방조치 및 개인정보 보호가 구현되는지, 법적 요건을 준수하고 있는지, 위험도 개선을 위한 필요한 조치를 하였는지 등에 대한 입증 절차 마련 등이 포함되어야 한다. 만약, DPO가 지정되어 있는 경우, 컨트롤러는 영향평가 수행 시 DPO의 자문을 구해야 한다.

(4) DPO지정

컨트롤러와 프로세서는 GDPR 제37조 및 BDSG 제38조에 따라 DPO를 지정해야 한다. 다만 모든 사업체가 DPO를 지정할 필요는 없으며, 이는 사업체의 규모와 성격에 따라 달라진다. BDSG 제38조는 GDPR 제37조에서 규정하고 있는 DPO 지정의무 요건을 추가하고 있다. 즉, GDPR 제37조에 따라 ▲공공기관 ▲정보주체에 대한 정기적·체계적 모니터링을 해야 하는 조직 ▲민감한 개인정보의 대규모 처리가 기본 활동인 조직 중 어느 하나에 해당할 경우 DPO를 임

명해야 하며, 추가적으로 ▲개인정보의 자동화된 처리를 다루는 사람을 최소 20명 이상 지속적으로 고용하는 조직 ▲개인정보의 자동화된 처리를 다루는 사람이 20명 미만인 민간 기업의 경우에는 i)컨트롤러 또는 프로세서가 GDPR 제35조의 개인정보 영향평가에 따라 처리를 수행하거나 ii)개인정보를 전송, 익명 전송, 시장 조사 또는 의견 조사 목적으로 상업적으로 처리하는 경우 DPO를 지정해야 한다.

사. 개인정보 역외이전(Transfer)

BDSG는 제25조에서 주로 공공기관 간 개인정보 국외이전과 관련한 규정만을 두고 있을 뿐이며, 기타 개인정보 국외이전은 GDPR 제44조 이하가 직접 적용된다.

제3국 또는 국제기구로의 개인정보 이전은 EU집행위원회가 충분한 보안 체계를 가진 국가를 선별한 뒤 적정성 결정(Adequacy decision)을 통해 개인정보 이전 가능 국가로 결정한 경우 가능하다(GDPR 제45조). 이전 대상 국가 또는 국제기구의 정보보안 수준은 4년마다 재평가되는데, 만약 해당 국가 또는 국제기구가 적절한 보호 수준을 더 이상 만족하지 못한다고 판단하는 경우 EU집행위원회는 적정성 결정을 철회, 수정, 또는 중지할 수 있다.

만약 이전 대상 국가 또는 국제기구가 EU집행위원회의 적정성 결정을 받지 못한 경우라 할지라도, 컨트롤러 또는 프로세서는 적절한 안전조치(▲공공당국 또는 기관 간 법적 구속력이 있고 강제할 수 있는 장치 ▲GDPR 제47조에 따른 의무적 기업 규칙 ▲EU집행위원회 또는 개인정보 감독기구가 채택 또는 승인한 정보보호 표준조항 등)를 제공한 경우에 한하여 정보주체가 행사할 수 있는 권리와 유효한 법적 구제책이 제공되는 조건으로 제3국 또는 국제기구에 개인정보를 이전할 수 있다(GDPR 제46조).

그밖에, 적정성 결정 및 적절한 안전조치가 없는 경우에도 제3국 또는 국제기구로의 개인정보 이전이 예외적으로 가능한 경우가 있으며, GDPR은 해당 사유를 제49조에서 아래와 같이 열거하고 있다.

- ① 정보주체가 적정성 결정 및 적절한 안전조치가 없어 자신의 개인정보 이전 시에 발생 가능한 위험을 통보 받은 후, 정보 이전에 명시적으로 동의한 경우
- ② 정보주체와 컨트롤러 간의 계약 이행을 위해 또는 당사자의 요청에 따라 취해진 계약 전 사전 조치의 실행을 위해 이전이 필요한 경우
- ③ 정보주체의 이익을 위해 컨트롤러와 그 밖의 다른 개인 또는 법인 사이에 체결된 계약의 이행을 위하여 이전이 필요한 경우
- ④ 중요한 공익상의 이유로 이전이 필요한 경우
- ⑤ 법적 권리의 확립, 행사, 방어를 위해 정보이전이 필요한 경우
- ⑥ 정보주체가 신체적으로 불가능하거나 법적으로 동의할 수 없는 경우, 정보주체 또는 타인의 생명, 건강 또는 재산을 보호하기 위해 필요한 경우
- ⑦ 정보 이전이 법률에 따라 정보를 공개할 목적이거나 일반 국민 또는 정당한 이익을 입증할 수 있는 제3자가 참조하기 위한 목적으로 만들어진 개인정보 기록으로부터 이루어진 것으로, 법률에 규정된 조건이 충족되는 범위 내에서 이전되는 경우

아. 집행

(1) 조사 및 시정조치

BDSG 제1부 제4장(제8-16조)은 개인정보 감독기구의 권한 및 의무를 규정한다. 개인정보 감독기구는 공공과 민간의 개인정보 처리 업무를 관리 감독한다. 감독기구 중 연방 개인정보 감독기구(BfDI, Bundesbeauftragte für den Datenschutz und die Informationsfreiheit)는 인사 및 예산의 독립성을 가지는 연방 최고의 독립제 기구이다. BDSG는 주로 BfDI 권한을 서술하며, 다른 16개 주 감독기구의 권한은 각 주 개인정보보호법에 근거한다.

감독기구의 업무는 GDPR 제57조와 동일한 취지로 BDSG 제14조에서 관련 내용을 규정하고 있으며, BDSG 제16조는 감독기구가 GDPR 제58조에서 규정하고 있는 권한을 갖는다고 명시하고 있다. 즉, 감독기구는 정보주체의 개인정보 보호와 관련된 일련의 조사 권한을 보유하며, 공공 및 민간부문이 GDPR 및 BDSG에 따라 적법하게 개인정보 처리를 할 수 있게 감독 및 시정조치 할 수 있는 권한을 보유한다.

(2) 과징금

개인정보보호 위반행위에 대한 처분 시 부과되는 과징금은 기본적으로 GDPR 제83조 규정을 따른다(2천만 유로 또는 전년도 글로벌 총 매출의 4%에 해당하는 금액 중 높은 금액). 이외에, BDSG는 소비자 대출과 관련하여 제43조에서 특칙을 규정하고 있다. 즉, BDSG는 제30조에서 소비자 대출을 허가하고 신용도 평가를 수행할 목적으로 개인정보를 처리하는 기관에 특별한 정보 제공 및 통지 의무를 부담케 하고 있는데, 감독기구는 이러한 의무사항을 위반한 기관에 대해 최대 5만 유로의 행정 과징금을 부과할 수 있다.

(3) 형사처벌

BDSG는 과징금 이외에도 개인정보보호 위반을 근거로 한 형사처벌 규정을 두고 있다(BDSG 제42조). 즉, 다수의 정보주체의 개인정보를 허락 없이 고의적으로 제3자에게 이전하거나 상업적 목적으로 이용할 수 있도록 하는 행위에 대해 3년 이하의 징역 또는 벌금에 처할 수 있다(제1항). 또한, 자신 또는 제3자의 이익을 추구하고 타인을 해할 목적으로 공개적으로 접근할 수 없는 개인정보를 허락 없이 처리하거나 부정 취득하는 경우에는 2년 이하의 징역 또는 벌금에 처할 수 있다(제2항).

4. 기타 관련 법령 : 통신 및 텔레미디어 개인정보 보호법(TTDSG)

TTDSG는 유럽사법재판소와 독일 고등법원이 정보통신 이용자의 명확한 동의를 받지 않은 쿠키정보의 이용이 EU법에 위반된다고 판시한 후 이러한 문제점을 해결하고자 정보통신법(TMG)과 텔레커뮤니케이션법(TKG)을 통합한 법률로, 정보통신 관련 개인정보보호 조항이 두 법률에 분산 규정되어 발생하는 법적 불확실성을 제거하고, GDPR 및 e-Privacy 규정(ePrivacy Regulation)과의 조화를 위해 2021년 5월 20일 독일 연방의회에 의해 승인된 법률이다. 동 법률은 2021년 6월 23일 개정된 전기통신법 시행령과 함께 2021년 12월 1일부터 시행에 돌입했다.

이에 따라, 쿠키(또는 이와 유사한 정보)를 설정하기 위해서는 GDPR 규정에 따른 최종 사용자의 동의를 요구되므로(TTDSG 제25조제1항), 무엇보다도 정보주체의 실질적이고(유효하고) 명시적인 동의가 필요하다. 다만, TTDSG 제25조제2항에서는 최종사용자의 동의를 요하지 않는 예외 사항을 다음과 같이 규정하고 있다.

- ① 최종 사용자의 단말기에 정보를 저장하는 유일한 목적이 공중 통신 네트워크로 메시지를 전송하는 것인 경우 (공중통신망으로 메시지를 전송하는 데 사용되는 쿠키)
- ② 텔레미디어 서비스 제공업체가 사용자에게 텔레미디어 서비스를 제공하기 위해 최종 사용자의 단말기에 정보를 저장하는 것이 절대적으로 필수적인 경우 (기술적으로 필수적인 쿠키)

서로 신뢰하고 함께 보호하는 개인정보

II. 행정체계

1. 개요

개인정보침해 민원 수렴 및 공공기관과 민간 사업체의 개인정보 처리를 관리 감독하는 기관을 개인정보 감독기구라 한다. 독일 내 개인정보 감독기구는 연방 개인정보 감독기구(BfDI, Bundesbeauftragte für den Datenschutz und die Informationsfreiheit)와 주(州) 개인정보 감독기구(LfDI)로 이루어져 있다. BfDI는 연방 정부 공공 기관을, 주 감독기구는 각 주의 공공기관을 관리 감독한다. 일반 사업체의 경우, BfDI는 통신 및 우편 사업체를 제외한 민간 사업체를 관리 감독하지 않는다. 일반 사업체는 소속된 주 개인정보 감독기구가 관리한다.

BfDI는 개인정보 보안 및 정보의 자유에 관한 연방 최고의 독립제 기구로, 1978년 1월 1일 설립되었으며, 본(노르트라인-베스트팔렌)에 위치해 있다. BfDI의 법적 지위는 연방 감사원과 유사하며, GDPR과 BDSG에 따라 민간 기업과 공공기관의 개인정보처리 수행을 자문하고 통제한다. BfDI는 2년 단위로 활동 보고서를 작성하여야 하며, 독립성이 보장된다.

감독기구를 이끄는 연방 커미셔너는 연방 총리실의 추천과 연방의회의 과반수 승인으로 선출된다. 연방 커미셔너는 BfDI 조직을 개편할 수 있으며 인사 독립성을 가진다. 현재 BfDI는 커미셔너 직속 부서와 총 4개 부서로 구성되어 있으며 추가로 독립기구인 중앙상담기관(ZASt)을 산하에 두고 있다. 연방 커미셔너 직속 부서는 BfDI 내부 DPO, 기밀보호 위임자, IT보안 위임자, 부패방지 담당자, 평등고용 담당자 등이다. 4개 부서는 중앙부서, 법과 국제부(1부), 정보자유법·기술적 개인정보보호·통신부(2부), 경찰과 언론부(3부)로 구성된다. BfDI 산하기관이지만 독립적으로 운영되는 ZASt는 BfDI와 독일 16개 주 개인정보 감독기구를 포함한 다른 유럽 국가 감독기구 간 협력이 용이하도록 힘쓴다. 2020년 BfDI 예산은 23,962,000 유로이며 약 250명의 직원이 BfDI에 소속되어 있다.

[그림 2] BfDI 조직도¹⁾



[표 2] 독일 공공부문 개인정보보호 감독기관

주(land)	개인정보 보호법 링크
연방 개인정보 감독기구 (BfDI)	전화: +49 228-997799-0 팩스: +49 228 99 77 99-5550 E-Mail: poststelle@bfdi.bund.de Homepage: https://www.bfdi.bund.de
바덴-뷔르템베르크 (Baden-Württemberg)	전화: 07 11/61 55 41-0 팩스: 07 11/61 55 41-15 E-Mail: poststelle@lfd.bwl.de Homepage: https://www.baden-wuerttemberg.datenschutz.de
바이에른(Bayern)	전화: 0981/53-1300 팩스: 0981/53-5300 E-Mail: poststelle@lda.bayern.de Homepage: https://www.lda.bayern.de
	전화: 089/21 26 72-0 팩스: 089/21 26 72-50 E-Mail: poststelle@datenschutz-bayern.de Homepage: https://www.datenschutz-bayern.de
베를린(Berlin)	전화: 030/13 88 9-0 팩스: 030/21 55 050 E-Mail: mailbox@datenschutz-berlin.de Homepage: https://www.datenschutz-berlin.de
브란덴부르크 (Brandenburg)	전화: 03 32 03/356-0 팩스: 03 32 03/356-49 E-Mail: poststelle@lda.brandenburg.de Homepage: https://www.lda.brandenburg.de
브레멘(Bremen)	전화: 04 21/361-2010 또는 04 71/596-2010 팩스: 04 21/469-18495 E-Mail: office@datenschutz.bremen.de Homepage: https://www.datenschutz.bremen.de/
함부르크(Hamburg)	전화: 040/428 54 - 4040 팩스: 040/4279 - 11 811 E-Mail: mailbox@datenschutz.hamburg.de Homepage: https://datenschutz-hamburg.de/
헷센(Hessen)	전화: 06 11/14 08-0 팩스: 06 11/14 08-611 E-Mail: poststelle@datenschutz.hessen.de Homepage: https://datenschutz.hessen.de/
메클렌부르크-포어포머른 (Mecklenburg-Vorpommern)	전화: 03 85/594 94-0 팩스: 03 85/594 94-58 E-Mail: info@datenschutz-mv.de Homepage: https://www.datenschutz-mv.de
니더작센(Niedersachsen)	전화: 05 11/120-45 00 팩스: 05 11/120-45 99 E-Mail: poststelle@lfd.niedersachsen.de Homepage: https://www.lfd.niedersachsen.de
노트라인-베스트팔렌 (Nordrhein-Westfalen)	전화: 02 11/384 24-0 팩스: 02 11/384 24-10 E-Mail: poststelle@ldi.nrw.de Homepage: https://www.ldi.nrw.de
라인란트-팔츠 (Rheinland-Pfalz)	전화: 061 31/208-2449 팩스: 061 31/208-2497 E-Mail: poststelle@datenschutz.rlp.de Homepage: https://www.datenschutz.rlp.de/

자란트(Saarland)	전화: 06 81/947 81-0 팩스: 06 81/947 81-29 E-Mail: poststelle@datenschutz.saarland.de Homepage: https://datenschutz.saarland.de/
작센(Sachsen)	전화: 03 51/493-5401 팩스: 03 51/493-5490 E-Mail: saechsdsb@slt.sachsen.de Homepage: https://www.saechsdsb.de
작센-안할트 (Sachsen-Anhalt)	전화: 03 91/81803-0 팩스: 03 91/81803-33 E-Mail: poststelle@lfd.sachsen-anhalt.de Homepage: http://www.datenschutz.sachsen-anhalt.de
슐레스비히-홀스타인 (Schleswig-Holstein)	전화: 04 31/988-1200 팩스: 04 31/988-1223 E-Mail: mail@datenschutzzentrum.de Homepage: https://www.datenschutzzentrum.de
튀링엔(Thüringen)	전화: 03 61/57 311 29 00 팩스: 03 61/57 311 29 04 E-Mail: poststelle@datenschutz.thueringen.de Homepage: https://www.tlfdi.de/

2. 역할 및 권한

BfDI와 주 개인정보 감독기구는 주로 공공과 민간의 개인정보 처리를 관리 감독한다. 개인정보 보안 관련 사항을 정리 및 배포해야 하며 개인정보에 대한 인식을 제고하는 역할을 수행한다. 이를 위해 개인정보보호와 관련한 사항을 교육하고 조언을 제공한다. 또한 정보주체의 개인정보 피해 관련 신고 및 민원 접수, 민원 해결 역시 감독기구의 역할이다. 감독기구는 독일 내 타 감독기구는 물론 다른 유럽연합 회원국 감독기구와도 협업해야 한다. 독일 내 16개 주 감독기구와 BfDI는 연방 및 각 주(州) 개인정보 감독기구 컨퍼런스(DSK)를 년 2회 개최하여 개인정보보호 관련 법률 및 행정 사항들에 관한 통일을 꾀한다.

모든 감독기구는 GDPR, BDSG, 각 주의 개인정보보호법에 근거한 행정 권한을 가진다. 이에 따라 감독기구는 사업체의 개인정보 처리를 감독하고 위반행위를 조사 및 처벌할 수 있다.

III. 피해구제 체계

1. 개요

정보주체는 자신의 개인정보에 대한 처리가 개인정보보호법을 위반했다고 여길 경우, 관할 개인정보 감독기구에 민원을 제기할 권리를 가진다. 관할 감독기구는 적절한 범위에서 민원 사항을 조사하고 진행 상황과 결과에 대해 정보주체에 대해 회신해야 한다.

감독기구에 민원을 제기할 권리의 법적 근거에 대해서는 BDSG가 침묵하고 있어 해당 권리는 GDPR 제77조에 기반한다. 동조는 GDPR 위반 행위에 대한 정보주체의 민원 제기 권리 및 관할 감독기구의 민원사항 조사 의무, 민원사항의 진행 상황 및 결과 통보 의무를 규정하고 있으며, 감독기구는 최대 3개월 내에 처리 현황을 정보주체에게 통보해야 한다.

정보주체는 자신의 거주지, 근무지 또는 침해행위 발생 의혹이 있는 회원국의 감독기구에 민원사항을 제출할 수 있다. 만약 다른 회원국의 개인정보 감독기구가 해당 민원 건에 대한 실질적인 권한이 있는 경우 민원을 접수한 감독기구는 타 회원국 감독기구와 긴밀히 협력하게 되며, 민원을 제기한 정보주체는 별도로 타 회원국 감독기구에 직접 연락을 취할 필요가 없다.

한편, BDSG 제60조는 범죄행위의 예방, 추적, 수사, 기소 또는 형벌의 집행을 위한 목적으로 개인정보를 처리하는 기관이 정보주체의 권리를 침해했다고 판단될 경우, 정보주체가 BfDI에 민원을 제기할 수 있다고 규정하고 있다. 이 때 개인정보를 처리하는 기관의 예로는 연방 정부기관, 고용센터, 통신회사, 우편회사, 보안 관련법의 적용대상 기업, 법정 의료보험 기관, 연금보험 기관, 사고보험 기관 등이 있다.

2. 처리실적

2020년 한 해 BfDI에 접수된 민원 건수는 총 7,878건으로 2019년 대비 약 5% 증가 했다. 정보보안 관련 사항에 대한 일반 민원이 주를 이루며(65%) GDPR 제77조 관련 민원이(38%) 그 뒤를 따랐다. 단순 민원과 별도로, 개인정보 유출 및 처리위반 신고 사례 역시 10,024건 접수되었다. 전년도 14,689건과 비교 했을 때 31% 감소했다. BfDI는 행정 조사 및 지도 사례 건수 역시 집계하였는데, '20년 기준 총 88건으로 전년도 124건에 비해 감소하였다.

2021년 10월 까지 독일은 유럽연합국가 중 다섯 번째로 빈번하게 과징금을 부과했다. 연방 및 각 주 감독기구는 2018년 GDPR 발효 후 2021년 9월 현재 까지 총 33건 과징금 행정처분을 내렸으며, 33건 과징금 총액은 약 5천만 유로이다. 과징금 총액 역시 유럽 국가 중 다섯 번째로 높은 수준이다. 가장 높게 부과된 과징금 액수는 35,258,708 유로로, 2020년 10월에 패션 사업체 H&M에 내려졌다. 해당 과징금 액수는 유럽 전체 과징금 액수 중 네 번째 높은 금액이며 H&M 독일 본사가 함부르크에 위치하기 때문에, 함부르크 개인정보 감독기구가 해당 행정 처분을 담당했다.

IV. Cases

1. H&M 함부르크

가. 개요

독일 함부르크 개인정보 감독기구(Hmb BfDI)는 스웨덴 의류회사 H&M 독일 서비스 센터 직원 개인정보 유출 혐의를 언론보도로 알게 되었다. 2019년 독일 서비스 센터 직원 개인정보가 시스템 결함으로 인해 회사 직원에게 유출되었고, 내부고발자 신고로 해당 사건이 언론에 알려진 결과였다.

함부르크 개인정보 감독기구는 조사를 통해 H&M 독일 서비스센터가 해당 직원 개인정보를 불법 수집 및 처리함을 파악 했다. 직원 동의 없이 개인 건강정보, 가족관계 등 사적 정보가 방대하게 수집되었다. 서비스센터 직원 약 600명 개인정보는 전산화되어 저장되었으며 데이터 크기가 약 60GB에 달했다. 감독기구는 해당 정보수집을 “과도한” 개인정보 수집 행위로 판단하고, 사건의 심각성을 감안해 높은 금액 과징금 약 3,525만 유로를 부과했다.

나. 함부르크 개인정보 감독기구의 조사

함부르크 개인정보 감독기구는 H&M이 침해한 GDPR 조항을 언급하지 않지만, 개인정보 침해 행위로 여겨진 H&M의 개인정보 수집 방식을 구체적으로 서술한다. H&M은 자사 직원 개인정보를 수집함에 있어 동의를 구하지 않았으며, 정보 수집의 목적과 무관한 개인 사생활 정보를 수집했다. 예를 들면, H&M은 휴가를 마친 직원 대상으로 “환영대화(Welcome Back Talk)”라는 절차를 운영했으며, 대화 중 오간 직원의 개인정보를 기록하였다. 또한 직원간의 사담을 엿듣고 건강정보, 종교, 성생활 같은 사생활 정보를 수집했다. 이에 더해 불법 수집된 직원 개인정보가 유출됨으로서 정보처리 내 요구되는 기밀성과 시스템의 무결성 역시 보호되지 못했다. 감독기구는 H&M의 이 같은 개인정보 수집을 “과도한” 개인정보 수집으로 여겼으며, 이 같은 개인정보 수집은 개인정보보호법을 심각히 무시하는 행위라고 종합적으로 판단하였다.

다. H&M의 대응

H&M 본사는 해당 개인정보 수집이 자사 가이드라인과 전혀 부합하지 않으며, 독일 뉘른베르크 서비스 센터의 단독 사고라고 발표했다. 뉘른베르크 서비스 센터의 개별적 행위임에도 불구하고 본사는 해당 사건의 문제를 책임지며 해당 사건 처리에 관하여 두 가지 대응 방안을 마련했다. 첫째로 H&M은 해당 사건 피해자에게 사죄 및 보상을 약속하였으며, 둘째로 개인정보 보안 시스템을 개편한다고 발표했다.

H&M 본사는 뉘른베르크 서비스센터 직원들에게 회사의 잘못을 전적으로 인정하고 공식적으로 사죄하며 GDPR이 시행된 2018년 5월 기준 이후의 개인정보 수집에 대한 보상금 지급 계획을 수립했다. 하지만 보상기간 측정에 관한 논

란이 있다. H&M은 정보 수집을 최소 2014년부터 시작했고, GDPR 시행인 2018 이전 피해 기간에 대한 보상은 약속하지 않았기 때문이다.

H&M은 해당 사건 지사 책임자와 정보보안 관련자 교체 및 보안시스템 강화를 추진한다고 밝혔다. H&M이 강구한 보안 시스템 강화 안건은 다음과 같다. 뉘른베르크 서비스센터 임원진과 DPO를 교체 하며 노동법과 개인정보보호법 관련 책임 임원진을 대상으로 추가 교육을 준비한다. 관리자들이 따라야 하는 가이드라인을 대폭 수정하며, 정보보호 시스템 관리를 다루는 추가 직책을 마련한다. 추가로 개인정보보호 시스템 체계를 전면 검토 및 보완한다.

라. 시사점

함부르크 개인정보 감독기구가 부과한 과징금 3,526만 유로는 독일 내 GDPR 관련 과징금 중 가장 높은 금액이다. 해당 금액이 부과된 2020년 10월 당시 유럽 내 두 번째로 높은 벌금 액수였으며, 2021년 10월 기준 네 번째로 높은 벌금액이다. 감독기구는 H&M이 해당 사건의 과실을 인정하고 개인정보 보안 시스템을 보완하려는 시도를 긍정적으로 평가하였으나, 개인정보 침해의 심각함을 기업에 고지하기 위해 높은 과징금을 부과했다.

과징금은 기업 전년도 매출 4%를 기준으로 했다. 여기서 매출액의 기준은 독일 H&M 전년도 매출이 아닌, H&M 세계 매출을 말한다. 해당 사건이 H&M 기업 전체 개인정보 처리 결함이 아니라, 오스트리아와 독일을 담당하는 뉘른베르크 서비스센터의 개별적 결함이었음에도 불구하고, 과징금 측정이 H&M 세계 매출을 기준으로 했다는 사실에 주의해야 한다. 즉 유럽 내 특정 국가의 사업규모가 작을지라도, 또는 개인정보 처리의 결함이 특정 지사에서 발생 할 지라도, 개인정보보호법과 관련한 과징금이 기업 세계매출과 비례하기 때문에 기업은 이에 막대한 피해를 입을 수 있다.

고객 개인정보가 아닌 직원 개인정보 처리 결함이 개인정보보호법 위반으로 여겨진다는 점 역시 주목해야 한다. 이같이 고객이 아닌 직원의 개인정보 처리 문제로 인해 행정 처분을 받는 사례는 H&M외에도 있다.(2019년 바덴 뷔텐부르크 음식회사, 2021년 전자제품 쇼핑몰 NBB) 유사한 성격의 개인정보 처리 결함으로 인해 빈번히 행정처분이 발생함을 고려했을 때 직원 개인정보 처리에도 주의가 필요하다.

2. 1&1

가. 개요

2019년 9월 독일 연방개인정보감독기구(BfDI)는 고객 개인정보 유출을 이유로 통신사업체 1&1에 개인정보보호 위반 과징금 995만 유로를 부과했다. 문제가 된 고객 개인정보 유출은 전화 상담에서 이루어졌다. 1&1은 전화 상담 시 고객 본인확인으로 성명과 생년월일을 물어보는 이중보안 시스템을 가졌다. 한 사람은 다른 사람을 사칭하여 해당 인물의 성명과 생년월일을 올바르게 답하여 본인확인에 성공하였고, 상담을 통해 고객 휴대폰 전화를 알아냈다. 해당 사건으로 전화번호 유출 피해를 입은 고객이 형사 고소했으며, 해당 사건이 연방 개인정보 감독기구에 전달되었다. 사건에 착수한 BfDI는 1&1이 지시하는 고객 본인인증 가이드라인이 지나치게 간소되었다고 지적하며 이를 개인정보 처리 보안 결함으로 판단하였다. 1&1의 과실은 인정되었으나 지나치게 높은 벌금 995만 유로는 행정처분이 내려진 1년 후 2020년 11월 항소재판에서 90만 유로로 낮아졌다.

나. BfDI 주장

GDPR 제32조 처리의 보안에 따르면 개인정보 보안은 무결하고 기밀을 지킬 수 있어야 한다. 즉 개인정보 처리는 무결한 보안 아래 이루어져야 한다. GDPR은 개인정보 보안을 위한 법적 의무로 제32조 제1항 제a)호에 개인정보의 가명처리 및 암호처리를 요구한다. 1&1은 위의 조항이 요구하는 본인확인 인증에 있어 결함을 지녀 고객 개인정보를 유출하였다.

따라서 BfDI는 본인 확인 인증 절차에 결함을 가져 제3자에게 고객 개인정보를 유출 한 1&1이 적절한 기술 관리 보안 조치를 마련하지 못했다고 판단했다. 또한 개인정보 유출 위험에 놓인 고객이 일부가 아닌 1&1 통신 서비스 가입자 전체에 달한다는 점 역시 심각한 위험으로 보았다. 2020년 기준 1&1 통신 서비스 가입자는 약 1,400만 명이다. 보안 결함으로 인해 개인정보 유출 피해에 놓인 정보주체의 수가 적지 않다는 점을 고려하여 BfDI는 과징금 995만 유로를 부과하였다.

해당 과징금액은 GDPR 제 83조 제4항 제a)호에 따라 전년도 세계 매출 2%를 기준으로 하였다. 4%가 아닌 2%라는 상대적으로 낮은 비율의 과징금은 1&1의 적극적인 수사 협조와 시스템 개선을 참작한 결과이다.

다. 1&1 주장

위반 사항과 벌금 책정 기준에 관해 1&1의 DPO는 반박 성명 했다. 1&1의 본인확인 인증 절차는 당시 업계 표준이었다고 해당 DPO는 주장했다. 또한 해당 사건이 GDPR이 발효된 해인 2018년 이전에 발생 했다는 점, 해당 콜센터 직

원이 당시 자사 개인정보 보안 규정에 따라 대응했다고 주장했다. 무엇보다도, GDPR 제32조에 명시된 “적정한 보안 수준 보장”에 있어 적절한 수준이 구체적으로 제시되지 않았다는 점을 지적했다. 당시 업계 평균 수준의 본인확인 절차가 “적정에” 달하지 못하는 보안 수준이냐고 반문하였다.

행정처분에 항의함과 동시에 1&1은 BfDI와 협력하여 보안시스템을 개편하기도 했다. 적정 보안 수준을 위해 고객 본인확인 인증절차를 기존의 이중 보안 절차를 삼중 보안절차로 개선하였으며, 또한 고객 개인 서비스 식별번호(Service-PIN) 시스템 역시 추가했다.

1&1은 개인정보보호법 전문변호사 하노 팀너(Hanno Timmer)와 우베 프레이슈미트(Uwe Freyschmidt)를 선임하여 높은 벌금 금액에 대해 항소했다. 변호사측은 낮은 수준 위반사항에 높은 벌금을 부과한 BfDI 행정처분이 균등대우 원칙과, 과잉조치 금지의 원칙에 충돌한다고 피력했다. 2021년 지방법원은 변호사 측 의견을 수용하여 벌금을 90% 이상 낮추어, 벌금 995만 유로를 90만 유로로 정정했다.

라. 시사점

1&1 사례는 높은 과징금이 항소재판을 통해 대폭 축소될 수 있다는 가능성이 증명된 사례이다. 개인정보보호법 위반 시 부과되는 높은 과태료 수준에 많은 기업이 비판하며 항의 하고 있기 때문에 해당 벌금 축소는 시사 하는 바가 크다. 이를테면 2021년 1월 독일 내 전자정보통신 및 매체 동업조합 비트콤(bitkom) 의장은 감독기구의 높은 과징금 책정을 공식성명으로 비판하였다. 동업조합 비트콤에는 약 2,700개 사업체가 소속되며, 이들의 연간 매출이 1900억 유로임을 고려한다면, 비트콤 의장의 발언은 GDPR 벌금 체계에 의미 있는 비판이라 볼 수 있다. 회사의 개선 의지를 참작하지 않은 높은 벌금은 사업체에 치명적인 재정적 피해를 입힌다는 점을 비트콤은 지적한다. 또한 순수익이 아닌 매출에 비례한 과징금 측정 원칙에 부당함을 주장한다. 기업이 의견을 모아 감독기구를 공식 비판하는 성명을 통해 많은 기업이 감독기구에 대한 불만을 가지고 있음을 알 수 있다.

벌금 축소에 있어 변호인 역할 역시 주목해야한다. 해당 사건을 변호한 팀은 다른 사업체 개인정보보호법 위반도 변호하며 GDPR 전문 변호인으로 활동 하고 있다. 이는 유럽 내 감독기구의 빈번한 행정처분과 높은 과태료 부과가 해당 분야 전문 변호사 성장을 초래했다는 점을 반증한다. GDPR에 특화된 변호사가 시장에 출현하면서 사업체가 항소재판에 승소할 가능성이 더욱이 높아졌다.

부록



부록 : 주요국 개인정보 감독기구 및 법제 현황

번호	국가	감독기구	법률	링크
1	미국	대표 감독기구는 없으나 연방거래 위원회(Federal Trade Commission, FTC)가 그 역할을 담당	FTC ACT 제5조(a)(1)	- FTC 홈페이지 (https://www.ftc.gov) - FTC Act (https://uscode.house.gov/view.xhtml?req=granuleid%3AUSC-prelim-title15-chapter2-subchapter1&edition=prelim)
2	일본	Personal Information Protection Commission (PIPC)	일본 개인정보 보호법 (PDPA)0	- PIPC 홈페이지 (https://www.ppc.go.jp/en) - 일본 개인정보 보호법(https://www.ppc.go.jp/en/legal)
3	대만	National Development Council (NDC)	대만 개인정보 보호법 (PDPA)	- NDC 홈페이지 (https://www.ndc.gov.tw/default.aspx) - 대만 개인정보 보호법 (https://law.moj.gov.tw/Eng/LawClass/LawAll.aspx?PCode=I0050021)
4	말레이시아	Department of Personal Data Protection (PDP)	말레이시아 개인정보 보호법(PDPA)	- PDP 홈페이지 (https://www.pdp.gov.my/jdpdv2/?lang=en) - 말레이시아 개인정보 보호법 (https://www.pdp.gov.my/jdpdv2/laws-of-malaysia-pdpa/personal-data-protection-act-2010/?lang=en)
5	태국	Personal Data Protection Committee (PDPC)	태국 개인정보보호법 (PDPA)	- PDPC 홈페이지 부재 - 태국 개인정보 보호법(https://www.dataguidance.com/sites/default/files/entranslation_of_the_personal_data_protection_act_0.pdf)
6	필리핀	National Privacy Commission (NPC)	필리핀 개인정보 보호법 (DPA)	- NPC 홈페이지 (https://www.privacy.gov.ph) - 필리핀 개인정보 보호법 (https://www.privacy.gov.ph/data-privacy-act/)

7	독일	Federal Commissioner for Data Protection and Freedom of Information (BfDI)	독일 개인정보 보호법 (DPA)	- BfDI 홈페이지 (http://www.bfdi.bund.de) - 독일 개인정보 보호법(https://www.gesetze-im-internet.de/englisch_bdsng/index.html)
8	러시아	Roskomnadzor	러시아 개인정보 보호법 (No. 152-FZ)	- Roskomnadzor 홈페이지 (http://eng.rkn.gov.ru) - 러시아 개인정보 보호법 (https://pd.rkn.gov.ru/authority/p146/p164/)
9	베트남	대표 감독기구는 없으나 - Ministry of Information and Communication (MIC) - Authority of Information Security (AIS), Ministry of Public Security (MPS) 등에서 분담하여 그 역할을 담당	대표 개인정보 보호법은 존재하지 않으며 - 베트남 사이버 정보보안법 (LCIS, Law on Network Cyberinformation Security) - 사이버보안법 (LOCS, Law on Cybersecurity)에서 개인정보 보호 항목을 규정	- MPS 홈페이지 (http://www.mps.gov.vn/) - MIC 홈페이지 (https://english.mic.gov.vn/Pages/home.aspx) - 베트남 사이버 정보보안법(LCIS) 영문(https://english.mic.gov.vn/Upload/VanBan/Law-on-Network-Information-Security-16-05-30.pdf) - 베트남 사이버보안법(LOCS) 영문(https://www.economica.vn/Content/files/LAW%20%26%20REG/Law%20on%20Cyber%20Security%202018.pdf)
10	싱가포르	Personal Data Protection Commission (PDPC)	싱가포르 개인정보 보호법(PDPA)	- PDPC 홈페이지 (https://www.pdpc.gov.sg) - 싱가포르 개인정보 보호법 (https://sso.agc.gov.sg/Act/PDPA2012)
11	영국	Information Commissioner's Office (ICO)	- 영국 개인정보 보호법 (DPA) - 영국 GDPR (UK GDPR)	- ICO 홈페이지 (https://ico.org.uk) - 영국 개인정보 보호법(https://www.legislation.gov.uk/ukpga/2018/12/contents/enacted) - 영국 GDPR(https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/969514/20201102_-_GDPR_-_MASTER_Keeling_Schedule_with_changes_highlighted_V4.pdf)

12	중국	Cyberspace Administration of China (CAC)	중국 개인정보 보호법 (PIPL)	<ul style="list-style-type: none"> - CAC 홈페이지 (http://www.cac.gov.cn/) - 중국 개인정보 보호법(원문) (http://www.npc.gov.cn/npc/c30834/202108/a8c4e3672c74491a80b53a172bb753fe.shtml) - 중국 개인정보 보호법(국문) (https://www.privacy.go.kr/pic/reference.do?divtype=2)
13	캐나다	Office of the Privacy Commissioner of Canada (OPC)	<ul style="list-style-type: none"> - 캐나다 개인정보 보호 및 전자문서법 (PIPEDA) - 프라이버시법(Privacy Act) 	<ul style="list-style-type: none"> - OPC 홈페이지 (https://www.priv.gc.ca/en) - 캐나다 개인정보 보호 및 전자문서법(PIPEDA) 원문(https://laws-lois.justice.gc.ca/eng/acts/p-8.6/FullText.html) - 캐나다 프라이버시법(Privacy Act) 원문(https://laws-lois.justice.gc.ca/ENG/ACTS/P-21/page-1.html)
14	프랑스	National Commission for Information and Freedom (CNIL)	- 프랑스 개인정보 보호법 (Loi 78-17)	<ul style="list-style-type: none"> - CNIL 홈페이지 (https://www.cnil.fr/en) - 프랑스 개인정보 보호법 (원문)(https://www.legifrance.gouv.fr/loda/id/JORFTEXT000000886460/)
15	호주	Office of the Australian Information Commissioner (OAIC)	- 호주 개인정보 보호법(Privacy Act)	<ul style="list-style-type: none"> - OAIC 홈페이지 (https://www.oaic.gov.au) - 호주 개인정보 보호법(원문) (https://www.legislation.gov.au/Details/C2021C00139)

서로 신뢰하고 함께 보호하는 개인정보