http://doi.org/10.36248/kdps.2020.14.3.099

보험업의 디지털화에 따른 개인정보의 활용과 보호에 관한 법적 과제
- EU GDPR 및 독일 보험업 정보보호행동강령과 비교를 중심으로 -

지 광 운*

<차례>

Ⅰ. 들어가며
Ⅱ. 보험업에 관한 개인정보이용 사례와 관련 법제의 내용
Ⅲ. EU GDPR 및 독일의 정보보호행동강령
Ⅳ. 고객정보의 활용과 개인정보 보호의 방향성에 관한 법적 과제
Ⅴ. 나가며

주제어 : 데이터3법, 빅데이터, 유럽일반정보보호법, 정보주체, 자율규제

<국문초록> 정보통신기술이 고도로 발달함에 따라 보험사업의 디지털화가 빠르게 진행되고 있다. 이러한 디지털화는 넓은 의미에서 보험회사측의 업무의 효율화를 촉진시킨다. 보험업의 디지털화가 진전되는 상황에서 개인정보의 활용은 보험회사에 상당한 메리트를 가져다준다. 그러나 고객정보가 보험회사측으로부터 유출되는 것을 어떻게 막는가 하는 보험회사의 고객정보관리에 관한 본질적인 문제가 제기된다. 나아가 신상품 개발에서 보험회사, 관련 계열회사 및 제휴회사는 어느 범위의 고객정보를 어느 정도까지 활용하는 것이 법적으로 허용되는지, 보험모집과정에서 보험회사, 보험대리점 및 모집인은 어느 범위의 고객정보를 어느 정도까지 활용하는 것이 법적으로 허용되는지도 문제가 된다. 특히, 빅 데이터를 활용하는 경우 정보는 누구의 소유인가라고 하는 문제도 제기된다. 이와 같이 상충되는 개인정보의 활용과 개인정보의 보호 양자를 어떠한 방향에서 조율해 가야 하는가는 중요한 법적 쟁점이 된다. 이러한 법적 쟁점과 관련하여 EU일반정보보호규칙(GDPR)의 내용은 상당한 시사점을 주고 있다.

2018년 5월에 시행된 GDPR은 우리나라의 개인정보보호법에 해당하며, 정보주체의 권리를 폭넓게 인정하고 사업자의 개인정보 취급에 관해 엄격한 의무를 부과한 법규제로서 알려져 있다.

* 충북대학교 강사, 법학박사(Dr.Jur & Ph.D).
- 논문접수일(2020.09.27), 심사개시일(2020.10.14), 게재확정일(2020.10.29)

GDPR 시행으로부터 2년 이상이 경과한 현재 GDPR이 규정하는 정보주체의 권리나 GDPR의 집행을 담당하는 정보보호감독 당국의 존재는 각 회원국에 따라 차이가 있지만, 일반적으로 사업자의 개인정보 처리와 관련하여 그 중요성에 대하여 관심도가 높아졌음은 주지의 사실이다. 개인정보를 사업자에게 제공하는 정보주체의 정보보호에 대한 인식이 향상됨에 따라 정보주체의 권리행사에 대한 대응 등 개인정보를 취급하는 개인정보취급자가 부담하는 의무의 이행은 더욱 중요해지고 있다.

보험회사도 개인정보를 취급하는 개인정보취급자로서 GDPR이 정하는 의무를 이행해 정보주체의 권리행사에 대응할 필요가 있지만, 삭제권 행사에 대한 대응을 비롯해 효과적으로 법 규제에 적응하지 못한 사례가 발생하고 있다.

본 논문은 유럽위원회가 GDPR 시행 1년 후에 실시한 조사 내용을 바탕으로 법 규제의 동향과 보험회사가 겪은 문제점과 향후 대처해야 할 과제를 소개하고, 이렇게 제기된 문제점을 독일의 보험협회가 제정한 정보보호행동강령을 통해 어떻게 대처하고 있는지에 대해 검토한다. GDPR은 유럽뿐 아니라 세계의 개인정보보호법 규제에 영향을 주고 있는 상황을 고려하면 GDPR을 둘러싼 과제나 동향은 우리나라 보험회사에게도 참고가 될 것으로 생각된다.

따라서 이에 대한 비교법적 검토를 통해 우리나라에서 개정데이터3법의 시행에 따라 변화가 예상되는 보험회사의 개인정보 취급과 관련한 법적 과제를 개인정보의 활용과 보호 사이의 균형성, 자율규제의 제정 필요성이라고 하는 측면에서 검토하였다.

Ⅰ. 들어가며

정보통신기술이 고도로 발달함에 따라 보험사업의 디지털화[1]가 빠르게 진행되고 있다. 이러한 디지털화는 넓은 의미에서 보험회사측의 업무의 효율화를 촉진시키지만, 보험 서비스 업무에 대해도 그 예외는 아니다. 예컨대 보험회사측이 이른바 어플리케이션을 통해서 계약 체결시에 설명하는 등, 전자 매체를 활용해 보험계약을 체결한다. 이 경우 다양한 고객정보를 전자매체 등에 기록한다. 그리고 보험회사측은 이러한 고객정보를 활용함으로써 고객에 대해 보다 적절한 보험 서비스 또는 보험 정보를 제공하는 것을 가능하게 한다. 이것은 고객 측에도 이익이 된다. 그러나 한편, 고객정보가 보험회사측으로부터 유출되는 것을 어떻게

1) 이 논문에서는 디지털화를 디지털 기술과 데이터를 활용한 사회 변혁의 개념으로 파악하기로 한다. 따라서 보험업의 디지털화란 전통적인 보험산업과 진화하는 디지털 기술의 접목 나아가 방대한 양의 데이터를 활용해 변화된 사회에서 보험산업이 경쟁력을 갖추는 과정으로 정의한다.

막는가 하는 보험회사측의 고객정보관리에 관한 본질적인 문제가 제기된다. 나아가 신상품 개발에서 보험회사, 그룹회사 및 제휴회사는 어느 범위의 고객정보를 어느 정도까지 활용하는 것이 법적으로 허용되는지, 보험모집과정에서 보험회사, 보험대리점 및 모집인은 어느 범위의 고객정보를 어느 정도까지 활용하는 것이 법적으로 허용되는지도 문제가 된다. 특히, 빅 데이터를 활용하는 경우 정보는 누구의 것인가라고 하는 문제도 제기된다. 이와 같이 상충되는 개인정보의 활용과 개인정보의 보호 양자를 어떠한 방향성에서 접근할 것인가는 법적 과제가 된다.

본고는 이상의 문제의식 하에 보험사업의 디지털화를 추진함에 따라 발생할 수 있는 고객정보의 이용·활용 및 보호의 방향성에 관한 법적 과제를 고찰하는 것이다. 이를 위해 2016년에 제정되고 2018년에 시행된 유럽 일반개인정보보호규칙(General Data Protection Regulation: 이하 GDPR)을 비교법적으로 검토한다. 해당 규칙을 통해 개인정보주체의 정보주권이 강화되었고 개인정보가 효과적으로 이용·활용되기 위해서는 개인의 프라이버시 보호와 사업자측의 이용·활용 사이에서 적절한 균형을 확보해 나가는 것이 중요하다는 인식하에 정보보호와 활용 양자 사이에서 균형적인 시각에서 다양한 제도를 규정하고 있는데 향후 우리나라의 경우에도 이와 같은 방향성에서 데이터 활용과 보호 법제가 구축될 필요가 있다고 본다. 이러한 문제의식 아래 이하에서는 보험업과 관련하여 중요성이 인정되는 GDPR의 주요규정과 시행 후 보험업계에서 과제로 인식하고 있는 내용 및 독일에서 보험업에 적용되는 정보보호행동강령(Datenschutzkodex)을 소개하고 우리법제와 비교를 통해 시사점을 도출한다.

Ⅱ. 보험업에 관한 개인정보이용 사례와 관련 법제의 내용

1. 법개정 내용

데이터3법 개정안은 지난 1월 국회에서 의결됐으며 8월부터 시행되었다. 이번 개정안은 '가명정보와 익명정보의 활용 허용 범위를 설정'하고 본인신용정보 관리업인 마이데이터 사업을 허용하는 내용을 담고 있다. 즉, 과학적 연구나 통계 작성, 공익적인 기록 보존 등의 목적을 위해서는 '가명' 정보 활용이 허용돼 가명정보

데이터들은 데이터 전문기관에 전송, 통계나 빅데이터로 사용된다. 가명정보라면 개인식별정보가 공개되지 않아 개인정보 유출에 대한 우려도 크지 않다. 만일 가명정보나 익명정보를 이용해 특정 개인을 식별할 수 있게 하면 과징금이 부과된다.

또 마이데이터산업은 본인 신용정보관리업으로 특정 정보주체의 개인정보를 다양한 소스에서 수집해 정보와 관련 서비스를 제공하는 사업모델을 가리킨다. 이미 마이데이터산업을 하고 있는 일본의 경우, 공개에 동의하는 정보 주체의 정보들을 마이데이터뱅크가 집적해 여러 회사에 제공하고 정보공개에 동의한 정보주체는 현금이나 포인트 등을 제공받는다. 기업들은 마이데이터뱅크로부터 데이터를 사 맞춤형 서비스 제공이나 마케팅 등을 할 수 있다.

데이터3법 통과로 기관간 데이터를 결합하고 활용할 수 있는 만큼, 신규 보험상품 개발이나 인수검사 및 요율 개선 등이 용이해질 가능성이 있다. 정보주체가 제3자 제공동의 등 별도로 절차를 밟지 않아도 과학적 연구, 통계 작성, 공익적 기록보존 목적을 위한 정보 결합이 편해져 결합정보에 대한 접근성이 높아지기 때문이다. 이를테면 유병자보험처럼 기존에 보험이 제공되지 않았던 부분도 이해도가 높아져 새로운 보험을 만들 수 있는 길이 열리게 된다.[2] 다만 이는 어디까지나 고객의 건강정보에 해당하고 이러한 민감정보의 처리기준에 대한 명확한 기준의 마련이 필요해 보험회사차원에서 해당 정보를 활용함에 있어서는 더욱 시간이 필요하다고 할 것이다. 아울러 마이데이터사업으로 새로운 보험 판매채널로 개인 맞춤형 서비스가 활성화될 것으로 보인다.[3]

(1) 개인정보의 개념 및 동의의 범위 확대

개인정보는 성명, 주민등록번호 및 영상 등을 통하여 개인을 알아 볼 수 있는 정보 외에 "해당 정보만으로는 특정 개인을 알아볼 수 없더라도 다른 정보와 쉽게 결합하여 알아볼 수 있는 정보"로 구분했다. 효율적인 개인정보의 활용은 다양한 개인정보를 결합할 때 가능해지므로 개념의 명확화는 "다른 정보와의 결합의

2) 최창희/홍민지, 「빅데이터 활용 현황과 개선 방안」, 보험연구원, 2019, 27면.

3) 이러한 마이데이터사업을 통해 단순히 보험 계약을 비교하고 분석하는 수준을 벗어나 개별 진단이나 처방, 치료 내역은 물론 자산현황, 생활습관 등을 통해 맞춤형 서비스가 가능해 지기 때문이다. 또 보험사들이 마이데이터뱅크에 개인정보 제공을 동의한 사람들의 정보를 확인하고 계약을 분석하기 편해지는 만큼, 고객 유치 경쟁 역시 치열해질 전망이다.

용이성"을 고려한 개정이라 볼 수 있다.[4] 그리고 시간·비용·기술 등을 합리적으로 고려할 때 다른 정보를 활용하여도 더 이상 개인을 알아볼 수 없는 정보, 이른바 익명정보는 적용대상이 아님을 분명히 함으로써 익명정보는 자유롭게 활용이 가능하다.[5]

(2) 신용정보법상 정보의 활용 강화

신용정보법의 경우에도 가명정보의 도입 등 데이터 활용을 촉진하는 규정을 신설하였으며, 그 외에도 신용정보주체의 신용정보를 일정한 방식으로 통합하여 본인에게 제공하는 행위를 영업으로 하는 '본인신용정보관리업'을 도입하였다. 본인신용정보관리업은 마이데이터사업이라고도 하는데, 신용정보주체의 신용 관리를 지원하기 위한 목적이다. 신용정보주체는 자신의 계좌·결제·투자 등 모든 금융정보를 스마트폰 애플리케이션으로 관리할 수 있고, 사업자는 고객에게 최적의 금융상품을 추천하는 등 자산관리 및 신용관리가 가능해진다. 또한 신용정보주체의 권리 강화를 위해 '개인신용정보전송요구권', '자동화평가대응권'을 도입하였다. 개인신용정보전송요구권은 개인인 신용정보주체가 금융회사 또는 신용정보제공이용자나 공공기관에 본인에 관한 개인신용정보를 본인신용정보관리업자나 다른 신용정보제공이용자에 전송할 것으로 요구할 수 있는 권리이다. 자동화평가대응권은 개인인 신용정보주체가 개인신용평가회사나 신용정보제공이용자에 대하여 자동화평가의 실시 여부, 자동화평가 결과 및 주요 기준에 대한 설명요구 등을 할 수 있는 권리이다. 전반적으로 신용정보주체가 자신의 정보를 통제할 수 있는 권리 등이 강화되었다고 할 수 있다.

(3) 개인정보처리자 및 기업의 법적 책임 강화

개별 개인정보처리자가 과학적 연구의 목적으로 갖고 있는 가명정보를 다른 가명정보 등과 결합할 경우에 보다 정보활용의 가치가 증대될 수 있다. 이러한

4) 김영국, "헬스케어서비스 활성화를 위한 법정책 과제-빅데이터에 기반한 개인의료정보의 활용을 중심으로-", 「보험법연구」 제13권 제2호, 한국보험법학회 2019, 202면.

5) 개인정보보호위원회의 독립성 확보도 중요한 개정사항이나 해당 논문의 쟁점과는 큰 관련성이 없어 별도로 다루지 않았다.

활용 증대를 위해 서로 다른 가명정보 결합을 허용하는 규정이 마련되었다.[6] 이러한 가명정보에 대하여는 보호위원회 또는 관계 중앙행정기관의 장이 지정하는 전문기관이 서로 다른 가명정보의 결합 업무를 수행할 수 있다(개인정보보호법 제28조의3 제1항). 또한, 개인정보처리자는 전문기관의 장의 승인을 받아 외부로 결합된 정보를 반출할 수 있도록 하였다(개인정보보호법 제28조의3 제2항). 이와 같이 개정데이터3법에서는 전문기관을 통한 가명처리 및 정보 반출을 법제화 하였다. 다만 이를 위반한 경우 형사 처벌 또는 과징금을 부과함으로써 가명정보의 처리 및 활용 절차를 구체화 하였다. 가명정보의 처리나 데이터 결합 시 안전조치 의무를 부과하고 특정 개인을 알아볼 수 있는 행위를 금지하였다. 이를 위반할 경우 과태료나 형사처벌 외에 전체 매출액의 3%에 해당하는 과징금도 부과할 수 있도록 하였다(개인정보보호법 제28조의6).

2. 보험회사에 의한 개인정보이용 사례

보험회사 입장에서 정보주체의 개인정보는 보험계약체결 과정 보험계약 이행과정 등에서 필수적으로 필요하게 된다. 이와 관련하여 아래에서 살펴보는 사례는 개인정보보호법 개정 전 보험모집 과정에서 정보주체의 동의권 필요여부에 대한 내용이다. 법 개정 전이므로 정보주체의 동의권이 정보활용에 있어 중요한 요건임을 알 수 있는데, 법 개정 후에는 가명정보를 통해 보험회사가 고객의 개인정보를 활용할 수 있는 길이 열려 있으므로 보험회사가 직접 판매 내지 위탁판매를 하는 경우 통계작성, 과학적 연구, 공익적 기록 보존 등을 위해 정보주체의 동의 없이 가명정보를 활용할 수 있게 되었다. 다만 법 개정 전이나 재정 후에도 보험자 입장에서는 개인정보처리자로서 안전조치의무를 부담한다.

(1) 보험회사에 의한 통신판매

보험 상품의 가입이 텔레마케팅의 방식으로 권유되는 경우 이는 보험회사에 의한 직접판매로 볼 수 있다. 따라서 텔레마케터가 보험자[7]에 의해서 적법하게

6) 김영국, "개정 데이터 3법과 보험업의 과제-디지털 헬스케어서비스 활성화를 중심으로-, 「보험법연구」 제14권 제1호, 한국보험법학회, 2020, 500면.

7) 대법원 2016. 10. 27. 선고 2016다29890 판결. "실적이나 업무수행 불량 또는 업무운용수칙 등

수집된 개인정보를 활용해 보험 상품을 마케팅하는 경우에 정보주체에 대한 별도의 동의나 업무 위탁이 고지되지 않더라도 개인정보보호법에 위반의 여부가 문제될 수 있다. 그런데 텔레마케터와 보험자간의 종속관계가 존재하고 보험자에 의해 적법하게 수집된 개인정보를 활용해서 텔레마케터가 보험 상품을 권유하는 형태로 업무가 이루어지고 있으므로 해당 사안의 경우에 고객의 별도의 동의나 업무 위탁이 고지되지 않더라도 법위반사항이 발생하지 않는다.[8] 이와 같이 개인정보보호법 개정 이전에 보험회사는 고객의 개인정보를 활용하기 위해서는 엄격한 동의요건을 충족한 경우나 텔레마케팅과 같은 보험자의 직접판매에 해당하는 예외적인 경우에 한해 고객의 개인정보를 활용할 수 있었다.

(2) 보험회사가 보험모집인을 통해서 판매한 경우

보험사가 보험모집인이 보험계약을 체결을 유인하는 과정에서 고객으로부터 주민등록번호를 제외한 개인정보를 직접 제공하면서 보험가입설계서 발행에 구두로 동의한 경우 보험사업자 또는 보험모집인이 고객의 별도 동의 없이 개인정보를 수집하여 이용할 수 있는지가 문제될 수 있다. 관련해서 행정안전부는 "정보주체와의 계약 체결 및 이행을 위하여 불가피한 경우에 해당한다고 볼 수 있으므로 보험계약의 목적 범위 내에서는 별도의 동의 없이 민감정보 및 고유식별정보를 제외한 개인정보를 수집·이용할 수 있다고 유권 해석한 바 있다.[9] 또한 청약자가 보험사업자의 보험모집인에게 자신의 명함을 교부하는 행위에 명함에 기재된 정보를 사용해도 좋다는 동의가 내재되었는지가 문제된 사안에서 역시 행정안전부의 유권해석은 명함에 기재된 청약자의 개인정보를 이용하기 위해 별도의 동의를 받을 필요 없다고 하였다. 행정안전부의 유권해석에 의하면 보험계약의 목적 범위 내로 한정하고는 있으나 정보주체의 별도의 동의 없이 개인정보를 활용할 수 있다는 점을 명확히 했다는 점에 그 의의가 있다. 다만 민감정보 및

위반 시 부과된 제재 또는 불이익, 업무의 성격과 내용, 근무장소가 정해져있고 근무시간을 지키지 않을 경우 얻게 되는 실질적 불이익 등 여러 사정을 종합하면, 원고들이 피고회사에 근로에 대한 대가를 목적으로 종속적인 관계에서 근로를 제공하였다고 볼 여지가 충분하다.".

8) 이희옥, "빅테이터 환경에서 보험업상 개인정보의 보호와 활용", 「소비자문제연구(제50권 제2호)」, 한국소비자원, 2019. 8, 142면.

9) 행정안전부, 개인정보보호과-4375, 2011. 12. 11.

고유식별정보의 경우에는 개인정보보호법 개정 전이나 개정 후에도 엄격한 요건하에 활용될 여지가 있고 후술하는 바와 같이 건강정보와 같은 민감정보에 대하여 가명처리화에 관한 명확한 기준의 마련이 필요하다고 할 것이다.

(3) 보험자의 개인정보 보호조치의무

보험사업자는 고객의 개인정보를 안전하게 취급·관리함에 있어서 개인정보보호법 제29조에 따라 수집한 개인정보에 대해서 안전성 확보 조치 의무가 있다. 안전성 확보 조치 의무란 수집한 개인정보의 안전한 처리를 위해서 내부 관리계획을 수립해 시행하고, 개인정보에 대한 접근 통제 및 접근 권한의 제한조치, 개인정보를 안전하게 이용하는 조치, 개인정보의 안전한 보관을 위한 시설, 잠금장치 설치, 개인정보침해사고의 발생에 대응하기 위한 조치, 개인정보에 대한 보안프로그램의 설치 및 갱신 등 기술적 보호조치를 말한다(개인정보보호법 제29조 및 동법 시행령 제30조). 그리고 동법 제30조에 따라 보험사업자는 개인정보의 처리목적, 처리 및 보유기간, 개인정보의 제3자 제공에 관한 사항 등이 포함된 개인정보 처리방침을 수립하고 그 방침을 인터넷홈페이지에 지속적으로 게재해야 한다.

다음으로 보험사업자는 개인정보 보호책임자를 지정해야 하는 의무가 있다. 일정한 자격을 갖춘 자를 개인정보 보호책임자로 지정해 개인정보 처리에 관한 업무를 총괄하도록 해야 한다. 개인정보 보호책임자는 개인정보 보호 계획을 수립 및 시행하고 개인정보 처리 실태조사 및 개선, 관련한 불만의 처리 및 피해구제, 내부통제 시스템 구축, 교육계획 수립과 시행, 개인정보를 보호하고 감독하는 업무를 수행한다(개인정보보호법 제31조 및 시행령 제32조). 이밖에도 보험사업자는 정보주체가 개인정보에 대해서 열람·정정·삭제·처리정지를 요청할 수 있는 구체적 절차와 방법을 마련하고 정보주체가 알 수 있도록 공개해야 하는 의무가 있다(개인정보보호법 제35조, 제36조, 제37조) 이와 같은 보호조치를 이행하게 되면 보험사업자는 개인정보유출과 같은 사건들이 발생하는 경우 책임을 면할 수 있다.

3. 정리

보험업에 있어 고객의 개인정보의 취급은 필수적이다. 보험가입단계, 보험유지단계, 보험금지급단계 등 다 방면에서 고객의 개인정보가 필요하게 된다. 이렇게 보험회사가 취급하는 개인정보가 많고, 민감한 정보를 포함하고 있으므로 이를 효과적으로 관리할 필요가 있다. 앞서 살펴본 데이터3법 개정 전까지는 보험회사 입장에서 고객의 개인정보는 엄격한 요건하에 활용될 수 있었다. 그런데 디지털경제의 진전과 개인정보 활용의 중요성으로 인해 정보주체의 개인정보를 보호하면서도 이를 효율적으로 활용할 수 있는 길을 마련해 줄 필요가 있었고, 그 결과물이 개정 데이터3법이라고 할 수 있다. 개정 데이터3법을 통해 보험회사 입장에서 활용할 수 있는 고객의 개인정보가 다양해졌고 해당 정보를 활용해서 고객에게 적합한 보험상품을 권유할 수 있는 제도적인 길이 확보되었다고 할 수 있다. 그런데 역설적이게도 보험회사가 활용할 수 있는 고객의 개인정보가 늘어나는 만큼 정보보호주체의 정보주권에 관한 인식도 높아지고 있어 주요국에서는 개인정보의 활용과 보호 사이에 균형점을 찾기 위한 법제를 구축하고 있다. 이하에서 살펴보는 GDPR은 이를 반영하고 있는 대표적인 입법례에 해당한다. GDPR의 제정후 유럽의 GDPR과 회원국의 개인정보보호법제와 저촉되는 규정을 정비하고 있으며, 이러한 법률의 개정은 보험업에 있어서 상당한 영향을 끼치고 있다. 이하에서는 GDPR시행 후 유럽의 보험업계가 당면한 과제와 독일의 정보보호행동강령에 대한 검토를 통해 향후 우리나라에서 검토되어야 할 법적 과제에 대하여 논한다.

Ⅲ. EU GDPR 및 독일의 정보보호행동강령

유럽연합(European Union: 이하 'EU') GDPR은 유럽연합 내의 개인정보보호에 대한 권리라는 기본적 인권 보호를 목적으로 한 법규제로서 2018년 5월부터 시행되었다. 정보주체의 권리를 널리 인정하고 개인 정보취급에 관해 엄격한 의무를 부과하고 있다.[10]

10) Voigt P., von dem Bussche A. (2018) Rechte der betroffenen Personen. In: EU-Datenschutz-Grundverordnung (DSGVO). Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-662-56187-4_5.

EU 내 정보주체의 개인 정보를 취급할 때에는 GDPR이 정하는 정보주체의 권리를 보호하기 위한 각종 요건을 적용할 필요가 있으며, 보험회사도 보험 계약자 등의 개인 정보를 취급할 때에는 마찬가지로 GDPR의 규정을 고려하여야 한다. GDPR은 정보주체의 다양한 권리를 규정하고 있는 EU 내의 통일된 개인정보보호법 규제로서 EU 내의 정보주체에게 널리 인식되고 있다. 잘 알려진 바와 같이 프랑스의 정보보호감독당국(Commission Nationale del'Informatiqueet des Libertés: 이하 'CNIL')에 의해 5,000만유로의 과징금이 부과된 구글이나[11] 영국의 데이터 보호감독당국(Information)에 의해 5,000만유로(Information Commissioner's Office: 이하 ICO)에서 1억 8,339만 파운드의 과징금이 부과된 브리티시 에어웨이즈의 사례는 GDPR이 정하는 정보주체의 권리에 관한 인식과 권리행사의식을 한층 더 강화시킬 것으로 생각된다.[12][13] 다만 회원국마다 국내법화 정도의 차이, 법규제의 보호 대상인 정보주체도 자신이 가진 권리의 내용을 충분히 이해하지 못하는 경우 등 여전히 개인정보 취급자와의 정보주체 사이에서 혼란이 발생하는 경우도 발생하고 있다.

유럽위원회(European Commission)는 2019년 7월에 GDPR 시행 후 1년 동안 각 업계의 이해 관계자가 경험한 과제 등을 유럽의회 및 EU 이사회(The Council of European Union)에 제출하도록 하고 있다.[14] 보험업계에서는 유럽의 보험협회를 대표해 EIOPA((European Insurance and Occupational Pensions Authority)가 보험업계의 현황과 과제를 보고했다.[15]

11) Gregory Voss, After Google Spain and Charlie Hebdo: The Con-tinuing Evolution of European Union Data Privacy Law in a Time of Change,71BUS.LAW. 281, 283–84 (2015).

12) 과징금부과 기준에 대해서는 Martin et al. (2018): Das Sanktionsregime der Datenschutz-Grundverordnung: Auswirkungen auf Unternehmen und Datenschutzaufsichtsbehörden. Hrsg.: Michael Friedewald et al., Forum Privatheit und selbstbestimmtes Leben in der digitalen Welt, Karlsruhe: Fraunhofer ISI. 2019, S. 13.

13) 한편, 중소기업과 같이 실제로 개인정보를 취급하는 개인정보관리자 측에서는 GDPR이 요구하는 의무를 준수할 만한 인적·경제적 자원이 결여되어 GDPR이 요구하는 요건에 충분히 대처하지 못하는 현상도 나타나고 있다.

14) European Commission, MULTISTAKEHOLDER EXPERT GROUP TO THE STOCK-TAKING EXERCISE OF JUNE 2019 ON ONE YEAR OF GDPR APPLICATION Multistakeholder Expert Group to support the application of Regulation (EU) 2016/679 Report 13. 7. 2019, p. 6.

15) European Commission, Ibid. p. 6.

1. 각 회원국의 국내법화 상황

GDPR는 규칙(Regulation)이므로 EU회원국의 국내입법을 필요로 하지 않고 직접 효력을 미치지만,[16] 후술하는 특수한 개인정보취급이나 자동화된 의사결정에 불복할 권리 등에 관해 각 회원국의 국내법에 따르도록 규정하고 있다. 각 회원국은 이러한 규정에 대응하는 국내법을 신설·개정할 필요가 있지만, GDPR 시행 1년 후의 단계에서도 포르투갈, 그리스, 슬로베니아의 3개국이 국내법의 정비가 완료되지 않은 상태였다.[17] 유럽위원회도 국내법 정비 지연을 긴급 과제로 지적하고 있다.[18]

2. 보험업계의 GDPR 적용 과제

유럽위원회는 EU의 각 이해관계자에게 GDPR 시행 후 1년이 경과해 판명된 현황과 과제에 대해 조사를 실시하였다. 이하에서는 보험업계에서 주요 과제로 제시된 내용을 중심으로 살펴본다.

(1) 정보주체의 권리 행사와 관련한 과제

정보주체가 보험회사에 대해 권리행사를 하는 경우 대응 상황과 관련하여 직면한 과제에 대해 살펴본다. 먼저 정보주체로부터의 보험회사에 대한 권리행사

16) 프랑스에서는 GDPR의 규정을 적용하여 자동차 보험회사에 대하여 과징금을 부과한 사례가 있는데 이를 소개한다. 프랑스 정보보호감독당국(CNIL)은 개인에게 자동차보험을 제공하는 프랑스 보험회사에 2019년 7월 18일 18만 유로의 신규 제재를 가했는데, 이는 홈페이지 이용자의 개인정보를 적절히 보호하지 못한 사례에 해당한다. CNIL의 조사는 정보주체 자신의 계정에서 다른 고객의 개인 정보에 접근할 수 있었던 고객의 신고에 의해 진행되었다. 개인정보에는 운전면허증 사본, 자동차 문서 및 은행 식별 세부사항이 포함되었다. 이러한 데이터는 검색 엔진에 고객의 이름을 입력하거나 웹사이트의 URL 주소에 번호를 추가하여 직접 액세스할 수 있었다. CNIL은 문제가 된 보험회사에 이 상황을 시정하라고 명령했다. CNIL은 며칠 후 검사를 실시했는데, 개인정보가 유출되는 것을 막기 위해 취한 조치가 불충분하다는 점에 주목하였다. 또한 로그인 암호(생년월일)가 충분히 안전하지 않았으며, 회사는 문서에 접근하는 각 개인에게 적절한 권한이 부여되도록 보장했어야 했으나 이를 하지 않았다. 따라서 이러한 조치는 GDPR 제32조를 위반하여 웹사이트 이용자의 개인정보의 보안을 유지할 의무를 준수하지 않은 것으로 보고 이에 대해 과징금을 부과했다.

17) 2019년 10월의 단계에서는 슬로베니아만 법안 단계에 있었다(access now, ONE YEAR UNDER THE EU GDPR AN IMPLEMENTATION PROGRESS REPORT, 2019, p. 9).

18) Ibid, p. 38.

상황에 대하여 EIOPA에서는 보험회사에 대한 정보주체의 권리행사 상황 및 그 대응상황을 다음과 같이 파악하고 있다.

정보 열람권에 대해서는 GDPR 시행 직후에 정보주체로부터의 권리 행사가 일시적으로 증가한 현상은 있었지만, 대부분의 보험시장에서 대폭적인 증가는 보이지 않고 약간 증가하고 있는 정도에 머물고 있다. 단, 프랑스,[19] 이탈리아[20] 등 일부 보험회사에서 정보열람권의 행사요구 건수가 전년에 비해 눈에 띄게 증가한 경우도 존재하고 있다.[21]

다음으로 삭제권과 관련하여 대부분의 회원국에서 삭제권의 행사 건수가 증가하고 있다. 보험계약 체결에 이르지 않고 보험 견적만 문의한 잠재고객에 의한 권리행사가 많은 것이 특징이다. 또한 계약을 체결한 지 얼마 안 된 정보주체로부터의 삭제권 행사도 많이 볼 수 있다.

EIOPA에 의하면 근거가 없거나 과도한 권리의 행사는 별로 없는 것으로 조사되었지만 보험회사가 실시한 삭제권의 대응에 불복해 정보 보호 감독 당국에 불만이 제기된 사례도 발생하고 있다.[22]

또한 정정권에 대해서는 GDPR 시행 후에도 거의 권리행사의 증가는 나타나지 않고 있다. 자동화된 결정에 불복할 권리와 정보이동권에 대해서는 대부분의 회원국에서 권리행사의 요구를 받고 있지 않다. 정보이동권에 대해서는 자동차 보험의 청구 이력의 이전에 관한 요구가 이루어진 케이스가 있었던 것이 보고되고 있다.[23]

이와 같은 정보주체의 권리에 대응해 보험업계가 당면한 문제는 다음과 같다.

---

19) 프랑스의 GDPR 국내법화 상황에 대해서는 Sonia Cisse, France - National GDPR Implementation Overview(https://www.dataguidance.com/notes/france-national-gdpr-implementation-overview), p. 8 이하 참조.

20) 이탈리아의 GDPR 국내법화 상황에 대해서는 Monica A. Senor, Massimo Durante, REPORT ON THE HARMONIZATION OF ITALIAN LAW WITH THE ENFORCEMENT OF THE EU GENERAL DATA PROTECTION REGULATION 2016/679(https://blogdroiteuropeen.files.wordpress.com/2018/06/italy.pdf), p. 6 이하 참조.

21) European Commission, IbId, p. 7.

22) 오스트리아의 보험회사가 데이터 주체로부터 보험계약 신청 시 제공한 개인 데이터를 삭제하라는 요구를 받은 사례. 요구받은 보험사는 삭제요구를 받은 데이터 중 일부를 삭제하고 나머지를 익명화했더니 데이터 주체에서 완전히 삭제요청을 충족하지 못한다고 오스트리아 데이터보호감독당국(DSB)에 민원이 제기된 사건이다. DSB는 익명화에 의해 개인의 추적 가능성은 제외되어 있으며, 데이터 삭제의 요청이 충족되고 있다며 정보주체의 요구를 거절하고 있다.

23) European Commission, Ibid, p. 7.

즉 대부분의 회원국에서 정보주체로부터의 권리행사의 요구에 대해 1개월 기한 내에 대응하는 것이 어려운 실태가 보고되고 있다. 그 요인으로 이하의 4가지가 보고되고 있다. 첫째, 권리행사 요구 건수가 증가한 점, 둘째, 정보주체로부터의 요구 내용이 복잡 한 점, 셋째, 열람권 행사 요구의 경우 제공할 필요가 있는 정보 정비에 시간이 걸린다는 점, 넷째, 정보주체의 권리행사 요구에 대응하는 시스템을 도입하지 않으면 수동으로 대응해야 하는 점이 문제점으로 지적되고 있다.[24]

또한 EIOPA는 정보주체의 삭제권 행사에 대응하는 디지털화의 과제로서 다음과 같은 점을 예로 들고 있다. 즉 장기 보험기간을 가진 보험상품도 있어 보험기간 종료를 제대로 식별할 필요가 있다는 점이 그것이다. 다음으로 삭제할 필요가 있는 데이터를 소정의 시간 내에 처리할 필요가 있다. 또한 보험회사뿐 아니라 대리점, 중개인이 가진 정보와 매칭할 필요가 있다. 그리고 보험수리상 계산을 하기 위한 이력 정보가 필요하며, 삭제되기 전에 데이터의 변환·보존 절차가 필요하다는 점을 거론하고 있다. 나아가 이러한 요건을 충족한 소프트웨어 및 IT솔루션의 개발이 필요하다는 점을 과제로 보고 있다.[25]

(2) 정보 열람권에 관한 과제

정보권에 관한 과제와 관련하여서는 보험회사가 정보주체로부터 개인정보를 수령했을 경우에 정보주체가 정보의 통지를 받을 권리에 관해 보험회사가 직면한 과제가 주된 논의의 대상이다.

정보주체는 개인정보관리자가 자신의 개인정보를 취득한 경우 및 정보주체가 열람권을 행사한 경우에 정보의 통지를 받을 권리를 가진다. 이에 대응해 정보를 취득한 개인정보관리자는 정보주체에게 개인정보관리자나 정보보호책임자의 연락처, 개인정보 취급이나 법적 근거, EU 역외 이전에 관한 정보 등을 기재한 정보를 통지해야 한다. 또 정보통지에는 통지를 실시하는 개인정보관리자 이외에 개인정보를 취득하는 공동관리자, 취급자나 제삼자등이 존재하는 경우는 해당 취득자의 명칭 또는 종류를 기재하여야 한다. 개인정보관리자는 정보주체에게 포괄적인

24) Ibid, p. 8.
25) Ibid, p. 8.

정보를 제공할 의무를 가지면서 동시에 그 정보를 간결하고 투명하며 이해하기 쉽고, 쉽게 접근할 수 있는 형식으로 제공해야 한다. 그 방법으로서 유럽 정보보호회의가 작성한 투명성에 관한 가이드라인에서는 디지털 환경에서 정보를 통지할 때 계층화 접근법이 권장된다.

계층화 접근법이란 정보주체에게 제공해야 하는 모든 정보를 단일 통지로서 제공하면 정보가 복잡해서 정보주체가 필요한 정보를 바로 확인할 수 없게 되는 사태가 우려될 경우 단일 통지로서 표시하는 것이 아니라 다양한 정보에 링크하는 계층적 프라이버시 통지를 이용하는 것이다.

정보주체가 최초로 적극적으로 접촉하는 제1단계에는 가장 중요한 정보인 취급의 목적, 개인정보관리자의 신원, 정보주체의 권리 설명 및 기타 정보주체에 미치는 영향이 큰 취급에 관한 정보가 기재될 것이 권장되며, 기타 계층의 정보는 정보주체가 필요한 정보가 어디에 있는지 명료하게 확인할 수 있는 설계와 배치가 이루어질 것이 요구된다.

EIOPA는 많은 보험회사가 프라이버시 통지를 수정하고 계층화 접근방식을 채택한 형태로 새로운 정보제공 의무에 대응하고 있다고 보고하고 있다. 한편으로 일부 정보보호감독 당국이 개인정보관리자가 계층적으로 정보를 제공할 때 사용하는 미디어를 변경하는 것을 피하도록 장려하고 있어 보험사 입장에서는 복잡하고 비용이 많이 드는 사태가 생겼다는 문제점도 지적되고 있다. 또한 정보권에 대해서는 정보주체가 보험계약 당사자가 아닐 경우, 이러한 정보통지의 의무를 다하는 것은 매우 어려우며 보험회사에 있어서 큰 부담이 된다는 지적도 존재한다.[26]

(3) 건강 데이터 취급에 있어서의 법적 근거에 관한 과제

이와 관련하여서는 개인정보를 취급하는 보험회사가 GDPR규정에 근거하여 어떠한 법적 근거를 가지고 개인정보를 취급하고 있는지 및 상해보험 등에서 취급하는 특수한 개인정보 중 하나인 건강정보 취급에 있어서 직면한 과제에 대해 살펴본다.

GDPR상 개인정보관리자의 개인정보 취급이 적법하다고 인정받기 위해서는 법이

26) KPMG, “The GDPR and key challenges faced by the Insurance industry”, KPMG’s Creative Services, 2018. 2.

정하는 법적 근거를 충족시킬 필요가 있다는 취지를 규정하고 있다(GDPR 제6조 제1항). 한편 특별한 종류의 개인정보는 원칙적으로 취급이 금지되고 있으나(GDPR 제9조 제1항), 일정한 법적 요건에 근거한 경우에는 취급이 인정된다(GDPR 제9조 제2항). 또 특별한 종류의 개인정보 중 유전 정보, 생체정보 및 건강정보에 대해서는 회원국의 국내법에 따라 해당정보의 취급의 법적 근거로 추가 내지 제한할 수 있다(GDPR 제9조 제4항).

EIOPA에 따르면 일반적으로 보험회사는 단체보험, 배상책임보험, 부정청구를 방지하는 차원에서 정보주체의 동의의 취득을 개인정보 취급에 관한 법적 근거로 삼는 것이 곤란하기 때문에, 개인정보를 취급하는 법적 근거로서 계약의 체결 또는 이행에 필요한 경우, 법적 의무의 준수에 필요한 경우 및 개인정보관리자 등의 정당한 이익에 필요한 경우에 의거해서 건강정보를 취급할 수 있는 것으로 하고 있다.

고객의 건강 데이터는 중요한 개인정보로 정보주체로부터의 명시적인 동의를 얻음으로써 건강정보를 취급하는 것이 가능하지만, 이하의 경우에는 동의 요건을 개인 데이터 취급의 법적 근거로 삼기가 어렵다는 문제점이 있다. 단체 상해보험의 경우 등 수집해야 할 개인정보를 가진 정보주체가 계약의 직접 당사자가 아닌 경우 보험사가 정보주체에게 개인정보가 필요한 이유를 설명해 동의를 얻어내기가 어렵다. 재보험 분야에서도 동일한 문제가 생긴다. 다음으로 배상책임보험의 경우 등에서 계약 당사자가 아닌 피해자에 대해 보험회사가 정보주체에게 개인정보가 필요한 이유를 설명하고 동의를 얻어내는 것이 어렵다. 또한 부정 청구를 방지·검출하기 위해서 건강정보를 취급할 필요가 있는 경우에 보험사기의 염려가 있는 정보주체로부터 건강정보의 이용의 동의를 얻는 것은 곤란하다.

또한 건강정보에 대해서는 GDPR 제9조 제2항에서 정해져 있는 법적 근거 이외에도 회원국의 국내법에 따른 취급이 인정된다. EIOPA에 따르면 이러한 배경으로 인해 건강정보를 적법하게 취급할 수 있는 법적 요건에 대한 고려가 회원국 간에 다르다는 점에 대하여 보고하고 있다.

EIOPA는 앞에서 기술한 보험회사에서 동의를 요건으로 하는 것이 어려운 경우가 있는 동시에 건강정보 취급에 관한 과제로서 다음과 같은 점을 보고했다. 먼저 건강정보 취급에 관해서 회원국간에 취급이 다르기 때문에 복수의 회원국간에 사업을 실시하는 보험 회사로서는 법규제의 준수가 곤란하다. 특히 재보험 분야에서

국내법의 규정이 없으면 원수보험회사와 마찬가지로 건강정보 취급에 대한 법적 근거가 필요하기 때문에 회원국 간의 개인정보 취급의 차이는 재보험회사가 여러 회원국에서 사업을 실시하는 것에 큰 제한이 될 가능성이 있다. 또한 고객이 건강정보 취급에 명시적인 동의가 필요한 것을 인지하지 못하고 있어 고객의 불만과 답변이 늦어지는 경우가 생기고 있다.

(4) 중개사업자와의 관계에서의 과제

GDPR에서는 개인정보관리자가 자신 대신 사업자(취급자)[27]에게 정보를 취급하도록 하는 경우에는 사전에 서면에 의한 계약을 체결하고, 취급자가 준수해야 할 보안 대책에 관한 의무나 정보주체의 권리 행사에 있어서 개인정보관리자에게 협력할 의무 등을 정하도록 요구하고 있다(제 28조 제1항). EIOPA는 보험회사와 보험회사로부터 업무를 위탁 받는 외부사업자 사이에 다음과 같은 문제가 발생하고 있음을 보고하고 있다.

보험시장에서 일반적으로 보험회사, 보험중개사업자, 재보험회사 등 복수의 시장관계자는 각각 자신의 서비스 제공과 고객관리를 위해 개인데이터를 취급하기 위해 각각 독립된 개인정보관리자에 해당한다. EIOPA는 일부 보험시장에서 이들 시장 참여자의 분류에 대해 어려움에 직면한 실태를 보고하고 있다.

유럽 보험중개사업자연맹(European Federation of Insurance Intermediaries)이 소속된 유럽의 중소기업 사업자 단체인 SMEunited에 보고한 내용에 따르면 일부 보험회사가 보험중개사업자를 일률적으로 취급자로 분류하고 있으며, 보험중개사업자와의 사이에서 긴 협상이 발생하고 있는 경우가 존재하고 있다.[28] 또한 유럽 보험중개사업자연맹의 측에서는 보험중개사업자는 보험회사와는 다른 개인정보관리자로 분류되어 보험회사, 보험중개사업자 모두 한쪽이 각각의 업무에서 다른 쪽 정보를 처리할 경우에는 개인정보처리가 된다고 판단하고 있으며, 이러한 입장이 업계 내에서 공유할 것을 권장하고 있다.

---

27) 취급자란 개인정보관리자를 위해 개인정보을 취급하는 자연인, 법인, 공적기관, 행정기관 도는 그 밖의 단체를 말한다.

28) SMEunited “Multi-stakeholder expert group to support the application of Regulation (EU) 2016/679 SMEunited1 input to the QUESTIONS TO PREPARE THE STOCK-TAKING EXERCISE OF JUNE 2019 ON THE APPLICATION OF GDPR” (2019.4).

GDPR의 규정에 따라 유럽위원회는 개인정보관리자와 취급자의 계약으로 정하는 내용에 대해 표준계약조항을 마련할 수 있다(제28조 제7항). 유럽위원회의 표준계약조항 작성 필요 여부에 대한 질문에 대해 EIOPA는 각 보험시장에서 의견이 달라 명확한 합의가 이루어지지 않았다고 보고했다. 보험회사의 의견에는 계약의 권리의무를 표준화함으로써 상대방과의 협상의 부담을 감소시키는 점 등에서 이점이 있는 한편 외부 사업자와의 계약은 각각 독자적인 특수성이 있어 표준계약 조항의 내용을 추가하는 것은 곤란하다는 의견도 존재한다.[29]

3. 독일 보험협회의 정보보호행동강령(Verhaltensregeln für den Umgang mit personebbezogenen Daten)

(1) 개인정보보호 법제

독일에서 개인정보와 기본권의 관계가 연방헌법재판소에서 처음 언급된 것은 국세조사판결(国勢調査判決)이다.[30] 이 판결은 기본법 제1조 제1항과 결부된 동 제2조 제1항으로부터 정보자기결정권을 도출했으며 이후 독일의 정보자기결정권은 본 규정에 기초하여 헌법상의 권리로서의 가치를 부여받고 있다.

독일의 일반적인 정보 취급에 대해서는 GDG(일반정보법)에 의해 정해져 있지만, 개인정보로서의 데이터 보호에 대해서는 EU GDPR이 적용되면서 2017년 7월 5일에 개정한 독일 연방정보보호법(Bundesdatenschutzgesetz: BDSG)이 중심적인 역할을 수행하고, 여기에 추가하는 형태로 구체적인 데이터 취급 제한을 개별법으로 정하는 구조로 되어 있다.

보험업에 대하여는 독일 보험협회가 제정한 자율규제에 해당하는 정보보호행동강령이 중요한 의미를 갖는다. 따라서 이하에서는 해당 지침의 내용을 살펴보고자 한다. GDPR과 연방정보보호법 모두 유럽회원국 전체에 구속력이 있고, 독일의 경우 해당 규칙을 국내법화 하였다. 유럽의회는 소위 개방조항(Öffnungsklauseln)을 통해 EU 회원국들에게 추가적인 법률을 제정해서 특정 사실을 구체적으로 규정하도록 하고 있다. 물론 독일의 연방정보보호법(BDSG)과 같은 회원국의 국내법은 GDPR의 원칙에서 벗어나서는 아니된다.

29) European Commission, IbId, p. 21.
30) BVerfGE 65, 1

개정 연방정보보호법은 2017년 5월 7일 연방법률로 관보에 게재되었다. 연방정보보호법은 새로운 GDPR과 동시에 2018년 5월 25일에 발효되었다. 개정 연방정보보호법은 GDPR의 기본원칙을 보완하고 GDPR의 다양한 요건을 명시하고 있다. 앞서 설시한 바와 같이 GDPR에서 일부 규정에는 소위 개방조항 또는 구체화조항이 포함되어 있다. 이 조항들은 개별 회원국이 자체의 법적 규정을 이용하여 GDPR의 요구사항을 구체화, 명시 또는 수정할 수 있는 기회를 제공한다. 그러나 이러한 규정은 GDPR의 요건과 상충되어서는 안 된다. 독일 연방정보보호법 제2편은 GDPR 제2조에 따른 개인정보수집목적의 절차에 관해 규정하고 있다. 특히 제22조는 특수한 범주의 개인정보에 처리에 관한 규정을 두고 있다. 이는 민감한 데이터로 취급자가 어떠한 경우에 정보를 수집할 수 있는지에 대한 원칙적인 내용을 규정하고 있다. 즉 다음과 같은 경우 공공 및 민간 기관에 의해 특수한 범주의 정보를 수집할 수 있다. 첫째, 사회보장 및 사회보호의 권리에서 파생된 권리를 행사하고 관련 의무를 이행하기 위해 처리가 필요한 경우, 둘째, 예방의학의 목적, 직원의 작업능력 평가, 의료 진단, 보건 또는 사회적 의료의 제공, 의료 또는 치료의 제공 또는 보건 또는 사회 의료 시스템과 서비스의 관리 또는 보건 전문가와의 데이터 주체의 계약에 따른 처리, 그리고 이러한 정보의 경우는 의료 전문가 또는 기타 전문적 비밀 유지의 의무를 따르거나 그들의 감독하에 처리된다. 이와 같이 민감한 정보라고 하더라도 사회적인 필요와 국가의 보건 목적상 필요한 경우 해당 정보를 수집할 수 있도록 하고 있다.

생각건대 후술하는 바와 같이 독일의 보험업에서의 정보활용과 관련한 자율규제인 정보보호행동강령 제6조는 연방정보보호법 제22조의 규정을 보험업의 특성에 맞게 구체화하여 규정하고 있는 것으로 보인다.

(2) 보험업에 적용되는 정보보호행동강령

보험업에 대하여는 연방데이터보호법 BDSG가 적용되고, 업태의 특수성에 비추어 보험사업자에 의한 고객의 개인정보 처리와 관련하여 필요한 절차 등에 대하여는 독일 보험협회(Gesamtverband der Deutschen Versicherungswirtschaft e.V.: GDV)가 제정한 정보보호행동강령을 통해 자율규제를 모색하고 있다. 이 지침은 EU GDPR 제정 후 해당 지침의 내용을 반영하여 2018년 6월에 개정되었다.[31]

정보보호행동강령[32]은 개인정보를 이용함에 있어 가능한 한 추가 동의를 하는 것을 불필요한 것으로 보고 있다. 다만 건강정보와 같은 특히 민감한 유형의 개인정보의 처리와 광고나 시장 및 의견 조사의 목적을 위한 개인정보의 처리의 경우에 추가적인 동의가 필요하다. 의료 데이터와 같이 특히 민감한 유형의 개인 데이터를 독일 보험협회와 감독당국은 민간한 정보의 처리에 관한 표준설명서를 작성하여 이를 보험사업자가 활용하도록 하고 있다. 따라서 보험사업자에게는 개인정보 처리시 감독당국이 제정한 표준조항에 해당하는 동의서를 사용할 것이 요청된다. 또한 해당 행동강령은 보험업계에 대해 정보보호규제의 내용을 구체화하고 보완한다. 정보보호행동강령은 독일 보험협회 회원사에게 적용되는 특별규정으로서 보험계약의 체결에서 종료, 법적 의무의 이행과 관련하여 중요한 개인정보의 처리에 관한 내용을 포함하고 있다. 해당 정보보호행동강령은 모든 회원사의 정보처리와 관련하여 적합해야 하기 때문에 가능한 일반적으로 적용할 수 있도록 공식화됨에 따라 개별 기업이 기업별 규제의 내용을 구체화할 필요가 있을 수 있다. 이와 같이 개별 기업별로 정보보호 기준을 설정할 수 있다고 하더라도 이러한 개별규제는 정보보호행동강령을 통해 달성되는 정보보호 및 정보보안 수준에 미치지 못하여서는 아니 된다. 즉 기업은 정보보호법(예: 건강 데이터와 같은 특히 민감한 정보나 인터넷 상의 데이터 처리를 위한) 측면에서 개인정보보호에 관한 더욱 강력한 개별규제를 자유롭게 제정할 수 있다. 회원사가 그러한 특별히 데이터 보호 친화적인 규정을 이미 도입하였거나, 특히 정보보호 준수 절차에 대해 관할 감독 당국과 특별한 합의나 협정이 있는 경우, 해당 개별규제는 정보보호행동강령의 제정에도 불구하고 그 유효성이 인정된다.

---

31) 해당 정보보호행동강령의 근거규정은 (구)독일 연방정보보호법 제38a조(2018년 5월 25일 까지 존치)였으나, 개정된 연방보호법에는 동일한 근거규정을 두고 있지 않다. 해당 규정의 내용의 원문은 다음과 같다. 다만 아래의 각주 30)에서 보는 바와 같이 GDPR상 지침의 제정의 근거규정이 존재한다.
§ 38a
Verhaltensregeln zur Förderung der Durchführung datenschutzrechtlicher Regelungen
(1) Berufsverbände und andere Vereinigungen, die bestimmte Gruppen von verantwortlichen Stellen vertreten, können Entwürfe für Verhaltensregeln zur Förderung der Durchführung von datenschutzrechtlichen Regelungen der zuständigen Aufsichtsbehörde unterbreiten.
(2) Die Aufsichtsbehörde überprüft die Vereinbarkeit der ihr unterbreiteten Entwürfe mit dem geltenden Datenschutzrecht.

32) 해당 지침의 GDPR상 근거는 Section 5 Codes of conduct and certification Article 40 Codes of conduct이다.

(3) 정보보호행동강령의 주요 내용

1) 정보처리의 목적에 관한 내용

정보보호행동강령은 정의 규정을 두고 일반 규정을 통해 개인정보 처리와 관련한 내용을 규정하고 있다. 먼저 일반규정 제1조는 적용범위에 대하여 규정하고 있고 제2항에서는 정보처리의 목적에 대하여 규정하고 있다. 먼저 강령 제2조 제1항에 따르면 고객의 개인정보는 보험관계의 설정, 이행 및 종료, 특히 신청의 처리에 필요한 범위, 보험계약법에 따른 자문업무의 이행, 수행의무의 심사, 청구권의 적기결산의 내부심사를 위하여 보험에 가입할 위험을 평가하기 위한 범위 내에서만 보험업무의 목적에 따라 취급되어야 한다. 또한 고객의 개인정보는 책임보험에서 피해자의 청구에 대한 심사와 규율, 구상권의 심사와 거절, 재보험계약의 체결과 이행, 보험요율, 상품, 서비스의 개발, 통계의 작성, 사고연구와 같은 보험관련 연구목적, 남용행위의 차단 또는 법적 의무의 이행, 광고 목적 및 시장의 의견조사를 위해 활용될 수 있다.

2) 정보처리의 기본원칙

정보보호행동강령 제3조는 정보처리의 기본원칙에 대하여 규정하고 있다. 즉 보험자는 모든 개인정보를 적법하고 투명한 방법으로 처리하며, 정보주체의 정당한 이익에 부합하는 방식으로 처리하여야 한다(정보보호행동강령 제3조 제1항). 또한 제2항에서는 최소활용의 원칙을 규정하고 있다. 즉 정보의 처리는 정보의 최소화와 저장의 제한이라는 목적에 부합하여야 한다. 이에 따라 EU GDPR 제5조 제(1)항 (e)에 의한 연구 및 통계목적으로 활용하기 위한 개인정보는 개인정보가 처리되는 목적에 필요한 경우 즉 정보의 저장이 정보처리에 필요한 경우와 같이 정보주체의 식별을 허용하는 형태로 저장되어야 한다. 특히, 익명화와 가명화는 개인정보의 보호 목적과 관련하여 불균형하지 않은 경우에 가능하다. 이러한 경우에는 익명화가 가명화보다 우선적으로 고려되어야 한다. 또한 보험회사는 기존의 개인정보가 올바르게 저장되었는지, 필요한 경우 최신의 상태로 보관하고, 불완전한 데이터를 지체 없이 수정, 삭제 또는 처리가 제한될 수 있도록 모든 합리적인 조치를 강구하여야 한다(정보보호행동강령 제3조 제3항).

3) 특수 범주의 개인정보처리

독일의 경우 GDPR 제9조 제1항에 따른 건강정보의 취급은 원칙적으로 금지된다. 다만 GDPR 제9조 제2항에서 정하는 예외적인 경우에 해당하면 건강정보를 취급할 수 있다. 나아가 GDPR 제9조 제4항에 따라 회원국은 건강정보 취급에 관한 추가적인 규정을 국내법화 할 수 있도록 한 규정을 근거로 독일 연방개인정보보호법 제22조, 제27조에서 정하는 바와 같이 연구목적으로 건강정보를 취급할 수 있도록 허용한다.[33] 이러한 일반원칙을 바탕으로 정보보호행동강령 제6조는 특수 범주의 개인정보처리에 관하여 규정하고 있다.

EU GDPR에서 규정하는 특수 범주의 개인정보(특히 건강정보)는 법적 근거(특히 데이터 보호 기본 규정 제9조와 연계) 또는 제5조에 따른 정보주체의 동의와 함께 필요한 경우, 비밀준수의무를 바탕으로 수집되고 처리되어야 한다(정보보호행동강령 제6조 제1항). 정보주체는 명시적으로 이러한 데이터에 대하여 동의를 하여야 한다. 이러한 특수 범주의 개인정보는 법적 근거를 두고 취급될 수 있는데 특히 법적 청구권의 주장, 행사 또는 방어를 위해 필요한 경우에 해당 정보의 취급이 허용된다. 예컨대 책임보험에 가입한 피보험자와 피해자의 청구권 심사 및 처리의 경우 적용된다(정보보호행동강령 제6조 제2항). 또한 정보주체의 건강데이터는 법률적으로 규정된 청구권의 행사, 심사, 정산하기 위한 목적으로 정보주체 자신의 동의 없이 처리될 수 있다. 또한 회사의 청구권 심사 및 정산 등 정보주체에 보험금을 지급한 사회보장기관, 고용주 또는 민간의료보험회사의 구상권에 대한 심사와 처리를 위한 경우에 동의 없이 처리될 수 있다(정보보호행동강령 제6조 제3항). 그리고 의료나 예방에 필요한 경우 건강정보와 같은 특수 범주의 개인정보는 법적 근거내에서 취급될 수 있다(정보보호행동강령 제6조 제4항). 이와 유사하게, 건강정보의 취급은 특히 지원 서비스(예: 응급 호출 서비스, 해외로부터의 구급차 운송 또는 조정)의 경우, 물리적 또는 법적 이유로 동의를 할 수 없는 경우 정보주체 또는 다른 사람의 중대한 이익 보호가 필요한 경우 동의 없이 수집될 수 있다. 이러한 사람들에 대해 치료가 합의되었고, 보험사고가 발생했을 때, 예를 들어, 사고 후 의식을 잃은 사람에게 구급차 운송이 필요하기

33) Brandi, Schutz von Gesundheitsdaten, Informationen zum Datenschutz I Februar 2020, S. 2(https://mail.google.com/mail/u/0/?tab=rm&ogbl#inbox/FMfcgxwJXLfqFfFsjfWWzpvzxjKBgNfl?projector=1&messagePartId=0.1).

때문에 동의를 얻을 수 없는 경우에는 동의를 요하지 않고 건강정보가 취급될 수 있다(정보보호행동강령 제6조 제5항).

건강정보와 같은 특수 범주의 개인정보의 취급은 정보보호행동강령 제10조의 규정에 따라 통계 및 연구목적으로 법적 근거하에 허용된다(정보보호행동강령 제6조 제6항).

4) 정보주체의 동의 없이 정보수집이 가능한 경우

정보보호행동강령 제8조는 정보주체의 동의 없이 정보수집이 가능한 경우를 규정하고 있다.

즉 제8조는 정보주체의 동의 없는 개인정보 수집에 관한 규정으로 제1항에 따르면 보험관계의 수립, 이행 또는 종료와 관련하여 특히 보험금 청구에 대한 심사 및 처리에 필요한 경우에는 정보주체의 동의 없이 개인정보를 수집할 수 있다. 예컨대 단체보험의 경우 보험가입자가 이 경우의 정보주체에 해당한다. 또는 생명, 손해 보험의 경우 보험수익자(피보험자)의 정보 또는 책임보험의 경우, 피해자에 대한 정보 또는 목격자의 정보를 적절하게 사용한다. 또한 정보주체의 협조 없이 개인정보는 보험통계작성 보험료 산정과 같은 목적(해당 지침 제10조 제1항)을 위해 수집될 수 있다. 나아가 제3자의 건강정보 또는 유전자 정보의 수집은 필요한 경우 해당 당사자의 기밀유지의무의 준수 및 보험계약법(VVG) 제213조 및 유전자검사에 관한 법률(GenDG) 제18조에 따라 수집될 수 있다.

5) 자동화된 의사결정

정보보호행동강령 제13조에서 규정하고 있는 자동화된 의사결정은 정보주체에 대해 법적효과를 미치거나 유사한 방식으로 유의미한 효과를 미치는 자동화된 결정은 동조 제2항, 제3항 및 제4항에 규정한 요건 하에서만 행해져야 한다(제13조 제1항). 즉 정보주체와 보험계약을 체결하거나 이행하는 데 필요하거나 급부를 제공하는 데 필요한 결정은 자동화 될 수 있다. 특히 다음과 같은 경우에 적용된다.

첫째, 보험계약의 체결 및 조건에 대한 청약자 결정, 둘째, 보험관계에서 보험금 청구에 대한 보험계약자에 대한 결정, 셋째, 운전 행위별로 보상하는 자동차

보험의 할인의 경우와 같이 일정한 행위에 따라 보험요율이 달라지는 결정은 자동화 될 수 있다.

보험계약에 보험금 청구에 대한 자동화된 결정(예: 공동보험자 또는 책임보험에 가입한 피해자에 대한 결정)도 정보주체의 요청이 있는 경우 허용된다. 또한 정보주체의 명시적 동의를 얻어 자동화된 의사결정을 할 수 있다. 특수범주에 속하는 개인정보도 자동화된 의사결정에 의해서 취급될 수 있으나, 이 경우에는 정보주체의 동의를 필요로 한다. 다만 이러한 특수범주의 개인정보라고 하더라도 앞서 설시한 보험금 청구에 있어 정보주체의 요구가 있으면 정보주체의 동의 없이 자동화된 의사결정에 의해 취급될 수 있다.

이러한 정보보호행동강령과는 별도로 독일 연방정보보호법상 자동화된 의사결정에 관하여 보험업에 적용되는 특칙적인 규정을 두고 있다. 즉 연방정보보호법 제37조에 의하면 GDPR(EU) 2016/679 제22조 제2항 제a호 및 c호에서 규정한 예외 외에, 보험계약 및 보험계약에 따라 서비스를 제공하는 맥락에서의 의사결정에 대하여는 정보보호행동강령 제22조 제1항에 따른 자동화된 의사결정에 관한 규정이 적용되지 않는다고 규정하고 있다.[34]

6) 광고목적을 위한 정보 취급

정보보호행동강령 제18조 제1항에 따르면 개인정보는 EU GDPR 제6조 제(1)항 (a) 또는 (f)에 근거하고 부정경쟁방지법(UWG) 제7조에 준하여 광고 목적으로

34) § 37 Automatisierte Entscheidungen im Einzelfall einschließlich Profiling
(1) Das Recht gemäß Artikel 22 Absatz 1 der Verordnung (EU) 2016/679, keiner ausschließlich auf einer automatisierten Verarbeitung beruhenden Entscheidung unterworfen zu werden, besteht über die in Artikel 22 Absatz 2 Buchstabe a und c der Verordnung (EU) 2016/679 genannten Ausnahmen hinaus nicht, wenn die Entscheidung im Rahmen der Leistungserbringung nach einem Versicherungsvertrag ergeht und
1. dem Begehren der betroffenen Person stattgegeben wurde oder
2. die Entscheidung auf der Anwendung verbindlicher Entgeltregelungen für Heilbehandlungen beruht und der Verantwortliche für den Fall, dass dem Antrag nicht vollumfänglich stattgegeben wird, angemessene Maßnahmen zur Wahrung der berechtigten Interessen der betroffenen Person trifft, wozu mindestens das Recht auf Erwirkung des Eingreifens einer Person seitens des Verantwortlichen, auf Darlegung des eigenen Standpunktes und auf Anfechtung der Entscheidung zählt; der Verantwortliche informiert die betroffene Person über diese Rechte spätestens zum Zeitpunkt der Mitteilung, aus der sich ergibt, dass dem Antrag der betroffenen Person nicht vollumfänglich stattgegeben wird.

취급될 수 있다. 정보주체는 직접적인 마케팅 목적으로 개인정보를 사용하는 것에 반대할 수 있다. 이러한 경우 개인정보는 더 이상 이러한 목적으로 취급되지 않아야 하며 회사는 이를 이행하기 위해 적절한 기술적, 조직적 조치를 취해야 한다.

7) 정보주체의 권리

정보보호행동강령 제23조는 정보주체가 보험회사에 대해 자신의 정보가 올바르게 취급되고 있는지에 대한 정보를 청구할 수 있는 권리를 규정하고 있다. 또한 제23a조에 따르면 정보주체의 정보전송권이 인정된다. 이에 따라 정보주체는 본인이 제공한 개인정보, 본인 동의나 계약에 의한 처리, 자동화된 절차의 보조를 받아 처리가 이루어지는 경우에 자신의 정보를 보험자로부터 전송받을 수 있다. 나아가 정정권에 대한 규정을 두고 있는데 해당 지침 제24조에 따르면 저장된 개인정보가 부정확하거나 불완전한 것으로 판명되면 정보주체는 보험자에 대하여 해당 정보의 정정을 요구할 수 있다. 해당 지침 제24a조 처리제한권에 관한 규정에 따르면 논란이 된 정보가 정확성이 검증되어야 하는 경우 등 보험자는 정보주체의 요청에 따라 정보의 취급에 제한을 받는다. 다음으로 정보주체의 삭제권에 대하여 살펴본다. 정보보호행동강령 제24b조에 따르면 개인정보는 수집·처리가 처음부터 불가한 경우, 이후 발생한 사정으로 처리가 불가한 것으로 판명되거나, 처리 목적을 달성하기 위해 더 이상 회사가 필요하다고 인정되지 않는 경우에는 개인정보는 즉시 삭제되어야 한다. 이러한 정보주체의 권리가 주장된 경우 보험회사는 정보주체의 권리행사 요청을 받은 날로부터 1개월 이내에 가능한 한 신속히 이행하여야 한다.

4. 소결

EU의 GDPR은 유럽내 개인정보보호에 관한 일반법으로서 제정되어 시행되고 있다. 해당 법률 회원국에 직접 적용되며 몇몇 개방형 규정을 두어 회원국이 국내법을 통해 GDPR의 내용을 보완하도록 하고 있다. GDPR은 정보주체의 정보주권을 강화하면서도 디지털정보사회의 진전에 따른 개인정보의 활용을 위한 다양한 제도를 두고 있다. 이는 개인정보의 활용과 보호를 모두 강조한 법률로 세계적으로 높은 관심을 끌고 있다. 서로 상충되는 양자의 가치를 하나의 법률에

담아 정보주체의 개인정보가 활용될 수 있는 법적근거를 명확히 하고, 개인정보가 오·남용되는 것을 방지하기 위해 정보주체에게 각종 권리를 인정하고 있다. 이러한 GDPR이 유럽내에서 시행되면서 유럽 내 보험업계에도 상당한 영향을 끼치고 있어 EIOPA차원에서 GDPR 시행 후 보험업의 문제점과 과제에 대하여 보고서를 발간하였다. 이 보고서는 GDPR 시행 후 보험업과 개인정보보호 및 활용에 관해 의미있는 내용을 포함하고 있어 이를 검토할 필요가 있다. 한편 독일의 경우 GDPR 시행에 맞추어 자국 연방개인정보보호법을 개정하여 시행하고 있다. 해당 법률은 개인정보보호에 관한 일반법으로서 보험업에도 당연히 적용된다. 그런데 보험업의 특성상 고객의 개인정보 활용과 보호를 위한 실무적인 요청을 고려할 필요가 있으므로 독일 보험협회 차원에서 제정한 정보보호행동강령이 시행되고 있다. 정보보호행동강령에는 GDPR 및 독일 연방개인정보보호법에서 규정하고 있는 내용을 보험업에 맞게 구체화하여 규정하고 있는 특징을 보인다. 지침의 주요 내용을 살펴보면 보험업에서 개인정보활용의 목적에 관한 규정, 특수한 범주의 개인정보 취급에 관한 규정정보주체의 동의 없이 개인정보 활용이 가능한 경우, 자동화된 의사 결정, 정보주체의 권리 등에 대하여 상세히 규정하고 있다. 생각건대 독일의 해당 지침은 보험업의 특성을 반영한 자율규제의 성격을 갖고 있고, 개인정보보호에 관한 일반법만으로는 보험업에서 활용되는 고객의 개인정보의 활용과 보호에 충실 할 수 없다는 인식이 반영된 결과물이라고 생각된다. 이하에서는 EU GDPR의 내용과 독일의 정보보호행동강령과 비교를 통해 검토한 우리나라 보험업계에서 개인정보의 활용과 보호에 관한 법적 과제를 설명한다.

Ⅳ. 고객정보의 활용과 개인정보 보호의 방향성에 관한 법적 과제

1. 고객정보의 활용·보호 양자의 조화를 위안 법제의 구축

보험업에 있어서 고객의 개인정보 활용은 필수적이다. 즉 보험업에 있어 고객의 개인정보는 보험모집단계에서부터 위험의 보장 나아가 보험마케팅에 이르기까지 다양하게 활용되고 있다. 기존의 개인정보보호법제가 지나치게 개인정보주체의 개인정보 보호를 강조하여 빅데이터 시대에 개인정보의 활용이 제약되는 상황을

개선하기 위해 앞서 살펴본 바와 같이 개정 데이터 3법이 8월 5일부터 시행되었다. 이러한 측면에서 개정 개인정보보호 법제는 변화된 사회상황을 반영한 것으로 바람직한 입법으로 생각된다. 따라서 보험사업자는 가명처리된 고객의 개인정보를 활용하여 새로운 상품을 개발하는 등 고객의 개인정보를 다양한 형태로 활용할 수 있게 되었다. 다만 개정 개인정보보호법상 활용 가능한 개인정보의 범위에 대해서는 여전히 해석의 여지가 있고, 고객의 개인정보 활용이 필요한 경우라도 개인정보보호법 제3조 개인정보 보호 원칙 제1항과 신의칙상 개인정보의 활용은 필요 최소한에 그쳐야 한다는 내재적 한계를 고려하면 고객정보의 활용의 범위를 업계의 자율규제의 측면에서 지침을 통해 구체화 할 필요가 있다고 본다.

한편 앞서 살펴본 바와 같이 EU GDPR상 정보주체에게 인정되는 다양한 권리는 진정한 개인정보의 주체로서 사업자에게 상당한 부담을 주는 것으로 볼 수 있다. 그런데 이는 GDPR의 제정 취지에서 보면 합리적인 선택으로 보인다. 즉 해당 규칙의 제정목적은 익히 알려진 바와 같이 개인정보의 활용을 도모하면서도 개인정보를 보호하기 위함에 있다. 이와는 달리 우리나라의 개정 데이터3법의 경우 명시적으로 정보주체에게 일정한 권리를 인정하고 있으나, 정보주권의 강화 측면에서 보면 후술하는 바와 같이 EU GDPR상 규정되어 있는 정보이동권에 관한 명확한 규정을 둘 필요가 있다. 물론 개인정보를 취급하는 자가 부담하는 의무에 상응하여 정보를 제공하는 주체의 입장에서는 헌법상 개인정보자기결정권[35]에 입각하여 GDPR상 인정되는 각종 권리에 상응하는 권리를 행사 할 수 있는 것으로 해석할 수 있으나, 정보가 활용되면서 그 활용이 남용되는 경우 등에 구체적으로 정보주체가 구체적으로 어떠한 권리를 행사할 수 있는지에 대하여는 개인정보보호법상 명확히 규정할 필요가 있다. 따라서 개인정보보호법 제4조 정보주체의 권리에서 인정하고 있는 개인정보주체의 정보 열람권, 정정권, 삭제권 외에 EU GDPR상 정보를 제공받을 권리(제13조, 제14조),[36] 정보이동권(제20조),[37]

35) 대법원 판례는 헌법 제10조에 보장된 인격권과 헌법 제17조에 보장된 사생활의 자유의 적극적 개념에 입각하여 개인정보자기결정권을 도출하고 있다(대판 1998. 7. 24. 선고 96다 42789) 반면에 헌법재판소는 개인정보자기결정권의 헌법상 근거로는 헌법 제17조의 사생활의 비밀과 자유, 헌법 제10조 제1문의 인간의 존엄과 가치 및 행복추구권에 근거를 둔 일반적 인격권 또는 위 조문들과 동시에 우리 헌법의 자유민주적 기본 질서 규정 또는 국민주권 원리와 민주주의 원리 등을 고려할 수 있다고 할 것이다. 따라서 그 헌법적 근거를 굳어 어느 한 두 개에 국한시키는 것은 바람직하지 않은 것으로 보이고, 오히려 개인정보 자기결정권은 독자적 기본권으로서 헌법에 명시되지 아니한 기본권이라고 보아야 한다고 했다(헌재 2005. 5. 26, 99헌마513).

자동화된 결정(프로파일링 포함 제13조)[38]과 같은 규정을 우리나라의 개인정보보호법제에 마련할 필요가 있다.[39] "선언적인 조항들을 열거적으로 두는 것이 실질적인 개인정보보호가 되는 것은 아니"라는 비판이 제기될 수 있다. 그러나 개정전 개인정보보호법은 정보주체의 개인정보자기결정권이 "동의권"을 중심으로 규정되었으므로 정보주체의 실질적으로 정보주체의 정보주권이 보장되는 형태는 아니었다는 점과, 기존의 동의권이 형식적인 동의로 여겨져 비판의 대상이 되었다는 점에서 보면 정보주체의 권리를 명시적으로 규정할 필요가 있다.[40]

먼저 정보를 제공 받을 권리에 대하여 살펴보면 향후 보험사업자인 보험회사가 마이데이터 산업에 참여해 서비스를 제공하는 경우, 정보주체가 언제든지 자기의 어떤 정보가 어떤 식으로 빅데이터 처리결과에 반영되는지에 대한 정보를 제공받을 수 있어야 한다.[41] 이는 GDPR의 프로파일링을 포함한 자동화된 의사결정 조항과 관련이 높은데 단순히 정보주체의 개인정보를 활용하는 것에 승인을 하는 차원이 아니라, 정보주체의 개인정보를 빅데이터화하는 것이 정보주체 어떻게 영향을 미칠 수 있는지에[42] 대하여 정보주체가 명확히 인식하도록 하여 정보주체의 정보주권을 강화하는 측면이 강하다.

다음으로 정보이동권에 대하여 살펴보면 GDPR 제13조 제1항에서는 정보주체로부터 개인정보를 수집하는 경우, 개인정보가 입수될 때 언제든지 이전의 동의를

---

36) 개인정보처리자는 "공정하고 투명한(fair and transparency) 처리원칙을 보장하기 위해 정보주체 에게 본인의 개인정보 처리에 관한 정보(information)를 어떻게 사용하고 있는지 알려주어야 한다. 이와 관련하여, GDPR은 개인정보처리자가 정보주체에게 제공하여야 하는 정보와 그 시기 및 방법에 대해 규정하고 있다. 이는 개인정보보호법 제20조(정보주체 이외로부터 수집한 개인정보의 수집 출처 등 고지)에 관한 규정과 유사하다. 다만 GDPR상 정보주체가 정보를 제공받을 권리에 대하여 좀더 세분화해서 규정하고 있음을 알 수 있다.

37) 정보주체는 개인정보처리자에게 제공한 자신에 관한 개인정보를 체계적으로 구성되고, 일반적으로 사용되며 기계 판독이 가능한 형식으로 제공 받을 권리가 있다. 또한, 그 정보를 다른 개인정보처리자에게 제공할 것을 요구할 수도 있다. 개인정보 이동권은 다음의 경우에 적용된다. 첫째, 정보주체가 개인정보처리자에게 제공한 개인정보로서, 둘째, 처리가 정보주체의 동의에 근거하거나 계약의 이행을 위한 것이며, 그리고 셋째, 처리가 자동화된 수단에 의해 이루어지는 경우 적용된다.

38) 정보주체는 ① 법적 효력을 초래하거나 ② 이와 유사하게 본인에게 중대한 영향을 미치는 사항에 대하여 프로파일링(Profiling) 등 자동화된 처리에만 근거한 결정 (automated individual decision-making, including profiling)의 적용을 받지 않을 권리를 가진다.

39) 이희옥, 앞의 글, 153면 이하.

40) 이희옥, 앞의 글, 153면 이하.

41) 이희옥, 앞의 글, 155면.

42) 이희옥, 앞의 글, 155면.

철회할 수 있음을 정보주체에게 제공해야 한다고 규정한다. 이는 정보주체가 자기의 개인정보를 제3자 또는 자기에게 이전해줄 것을 정보처리자에게 요구할 수 있는 권리인 정보이동권에 관한 규정이다. GDPR상 정보이동권은 우리나라의 개정 신용정보법 제33조의2 개인신용정보의 전송요구에 관한 규정과 유사하다. 동조에 따르면 개인인 신용정보주체는 신용정보제공·이용자등에 대하여 그가 보유하고 있는 본인에 관한 개인신용정보를 전송하여 줄 것을 요구할 수 있다. 그런데 이는 GDPR과는 달리 전송요구권의 대상이 정보주체의 신용정보에 국한하고 있어 개인정보 전체에 적용되는 GDPR의 정보이동권보다는 협소한 개념이다.[43] 정보주체의 정보주권을 강화한다는 측면과 국제적 정합성 측면 양자를 고려하여 현행과 같은 신용정보에 국한한 정보이동권에 관한 규정을 개인정보보호법을 통해 규정할 필요가 있다. 나아가 우리나라의 경우에도 정보주체의 자기 정보에 대한 적극적인 활용을 열어두는 것이라는 점에서 의미가 있는 정보이동권을 인정할 실익이 크다. 보험계약자 등의 계약정보 등은 보험회사나 신용정보집중기관에 독점되어 있었으므로 앞으로는 계약정보나 여타 개인정보에 있어서 정보주체의 권리의 일부로서 정보이동권을 인정할 필요가 있다. 이러한 권리를 정보보호 관련법에 포섭시키고, 보험사업자가 이와 같은 권리가 존재함을 안내 및 고지하도록 한다면 정보주체의 정보통제권을 강화하는데 도움이 될 것으로 본다.[44]

보험업의 경우 특히 보험계약의 체결, 이행 과정에서 개인정보를 활용할 여지가 크고, 보험금청구, 지급심사, 지급 과정에서 개인정보 처리를 위해 제3자에게 개인정보를 위탁하기 때문에 개인정보 활용에 관한 근거 조항을 개인정보보호법제에 별도로 둘 필요성이 크다.[45] 그런데 구체적으로 어떻게 개인정보보호법상 정보주체의 권리가 보험업에 있어서도 적용되도록 일반적인 규범화에 대한 고민이 필요하다. 개인정보를 취급하는 자인 보험사업자는 개인정보보호법을 준수하여야 할 것이고, 정보주체는 개인정보보호법상 자신의 권리가 인정된다고 하더라도 법규의 명확성 측면에서 어떠한 경우에 정보주체가 해당하는 권리를 행사할 수 있는 것인지에 대해 규정할 필요가 있다. 따라서 EU GDPR 제20조에서 보는

43) 황현아, 마이데이터 산업의 내용과 과제: 신용정보법 개정안을 중심으로, KiRi 리포트 2019.4.22., 10면.
44) 이희옥, 앞의 글, 153면 이하.
45) 이희옥, 앞의 글, 153면 이하.

바와 같이 정보주체의 동의와 계약의 이행에 필요한 경우에는 정보이동권이 인정되는 것으로 규정하는 형식을 통해 일반적인 정보주체의 권리가 보험업(계약)에 있어서도 적용된다는 점을 명확히 할 필요가 있다.

빅데이터 시대에 보험업자는 고객의 개인정보를 활용한 다양한 신사업과 새로운 상품을 개발하여 경쟁력을 확보할 필요가 있다. 보험사업자가 경쟁력을 확보하기 위해서는 정보의 활용에 지나치게 의존할 것이 아니라 고객의 개인정보를 보호하려는 노력도 병행하여야 변화된 디지털화 사회에서 경쟁력을 갖출 수 있다. 이러한 인식의 전환아래 보험사업자는 정보주체에게 인정되는 다양한 권리로 인해 사업자 입장에서는 이를 규제로 받아들여 정보활용에 제약이 될 수 있다는 부정적인 생각에서 벗어나 고객의 개인정보 활용 및 보호를 위해 필수적인 시스템을 구축할 필요가 있다고 본다. 이를 통해 고객의 신뢰를 기반으로 경쟁력을 이어나갈 수 있을 것으로 예상된다.

2. 보험업에서 민감정보 활용에 관한 자율규제를 통한 명확화

"자율규제"라 함은 협회와 생명보험회사가 자율적인 합의하에 운영하는 자체규제를 말하며 생명보험회사의 권리를 제한하거나 의무를 부과하는 것 또는 생명보험회사의 영업 또는 업무 등에 사실상 영향력을 행사하는 모범규준, 협약, 준칙, 지침, 가이드라인 등으로 운영세칙에서 정하고 있는 금융규제를 말한다.

이와 같은 민간의 자율규제 지침의 제정을 보험업계에 맡기는 규제체계를 생각할 수 있다.[46] 특히 개인정보 이용·활용의 구체적 방법은 각 업종·업태에 따라 다르며 법령에 의해 획일적이고 포괄적으로 규제하는 것에 익숙하지 않은 것도 있을 수 있다. 오히려 각 업종·업태 등의 특수성을 존중하고, 각각의 민간이 자율적으로 정하는 규제 룰에 맡기는 것이 개인정보를 보호하는 것에 이바지한다.

특히 민감정보의 처리와 관련하여 자율규제를 통해 해당 정보의 활용과 보호에 관한 명확한 기준을 마련하는 것이 시급하다고 할 것이다. 민감정보의 처리 특별법인 신용정보법에 따르면 신용정보회사 등은 질병정보 외의 민감정보를

46) 자율규제에 대한 비판적인 견해로는 사설 자율규제 대폭 정비해야 한다, 2019년 1월 7일자 보험신보 기사 참조(insweek.co.kr/45760).

수집하는 것이 금지된다. 이를 보험회사에 적용하면 보험회사는 질병정보 외의 민감정보는 개인의 동의를 받더라도 처리할 수 없는 것으로 해석하는 것이 합리적이다.[47] 다만 개인정보보호법 제23조 제1항 제2호에서 정하는 바에 따라 법령을 통해 민감정보의 처리를 요구하거나 허용하는 경우에 해당하면 보험회사가 민감정보를 처리할 수 있다.[48]

특히 정보주체의 민감한 정보인 건강정보에 대한 보험회사의 활용은 향후 헬스케어 산업의 활성화와 맞물려 상당한 파급력을 가져올 수 있다. 나아가 민감정보의 가명처리 기준이 명확히 마련되어 있지 않아 보험업계에서 고객의 건강정보를 이용한 새로운 상품의 개발이 어려울 것으로 예상된다. 이와 관련하여 가명정보에 대한 처리기준을 명확히 할 필요가 있다. 개인정보보호법 제28조의2(가명정보의 처리 등)에 따르면 개인정보처리자는 통계작성, 과학적 연구, 공익적 기록보존 등을 위하여 정보주체의 동의 없이 가명정보를 처리할 수 있도록 하였다(동조 제1항). 나아가 개인정보처리자는 가명정보를 제3자에게 제공하는 경우에는 특정 개인을 알아보기 위하여 사용될 수 있는 정보를 포함해서는 아니 된다(동조 제2항). 위와 같이 가명처리 합법화를 위한 기준과 방법을 일률적으로 법률을 통해 규정하기는 매우 어렵다. 앞서 개인정보보호법 제28조의2의 규정에 따르면 보험업과 관련이 있는 가명정보의 처리 근거는 통계작성에 가장 유사한 방법으로 이루어질 수 있는데, 해당 법문이 명확히 보험사업자에게 가명정보처리 기준을 제시하고 있는 것으로 해석하기 어려운 측면이 있다. 개인정보보호법이 고객의 개인정보보호와 활용에 관한 일반법이므로 법문의 의미는 조금 더 명확하게 규정될 필요가 있다. 그러나 해당 법문을 통해 정보를 취급하는 모든 산업에 적용되는 일반적인 기준을 마련하다 보니 통계작성, 과학적 연구, 공익적 기록보존 등을 한정적으로 열거하고 있어 법규의 명확성 측면에서 보면 부족한 면이 있다. 결국 이는 개인정보보호법이 정보보호와 활용에 관한 일반법으로서 작용한다고

47) 이희옥, 앞의 글, 153면.

48) 그밖에도 위탁 보험회사가 자신의 영업을 위하여 보험개인정보의 처리를 위탁하는 경우 정보주체로부터의 동의는 필요 없는 것으로 해석되나, 정보통신망법 및 개인정보보호법의 위탁 절차(위탁내용의 주기적 통보, 수탁자의 관리·감독 등)는 준수하여야 한다. 엄격한 동의주의가 적용 곤란한 보험거래의 경우는 정보주체가 계약당사자가 아닌 경우가 다수 존재하므로 현실적으로 동의 수령이 용이하지 않다. 따라서 사전동의를 엄격히 요구할 경우 보험회사 간 정보공유가 불가피한 보험의 특성에도 불구하고 보험정보의 수집 및 제공이 극히 제한되어 보험산업 전반의 위축을 초래할 가능성이 있다는 문제를 제기하는 견해도 있다(이희옥, 앞의 글 153면.).

하더라도 산업별 특성을 반영하지 못한다는 반증이므로 이를 개선하기 위한 측면에서 가명정보처리의 기준, 민감정보의 가명정보화 가능성 등을 업계가 제정한 자율규제내지 산업별 가이드라인을 통해 반영하려는 노력이 필요하다고 본다. 특히 민감정보에 포함되는 건강정보도 가명화해서 처리할 수 있는지 명확하지 아니하므로 건강정보도 가명처리 정보에 포함되는 것으로 보고 보험업에서 자율규제를 통해 그 활용기준과 개인정보보호 기준을 마련하는 것이 필요하다고 본다.

참고로 EU GDPR 제9조 제4항에 의하면 건강정보와 관련한 민감정보의 처리에 관한 법적근거를 정비하도록 회원국에 일임하는 개방규정형식을 취하고 있는 것이 특징이다. 따라서 회원국에서 정한 국내법에 따라 정보주체로부터의 동의 취득을 필요로 하지 않고, 보험회사가 건강 정보를 취급하는 것을 인정하고 있는 입법례가 있다.[49] 스페인에서는 영향을 받는 당사자의 보험계약 실행에 필요한 경우에 보험 분야에서 건강 데이터 취급을 인정한다는 내용이 규정돼 있다.[50] 아일랜드에서는 정보주체의 기본적인 권리와 자유를 보호하기 위해 적절하고 구체적인 조치가 강구되는 것을 조건으로 보험 분야에서 건강 데이터의 취급을 인정한다고 규정하고 있다.[51] 핀란드에서는 보험 분야에서 건강데이터를 사용할 경우 GDPR 제9조 제1항의 규정이 적용되지 않는다고 규정하고 있다.[52]

49) 앞서 살펴본 독일의 경우도 이 입법례에 해당한다.

50) Artículo 9. Categorías especiales de datos.
2. Los tratamientos de datos contemplados en las letras g), h) e i) del artículo 9.2 del Reglamento (UE) 2016/679 fundados en el Derecho español deberán estar amparados en una norma con rango de ley, que podrá establecer requisitos adicionales relativos a su seguridad y confidencialidad. En particular, dicha norma podrá amparar el tratamiento de datos en el ámbito de la salud cuando así lo exija la gestión de los sistemas y servicios de asistencia sanitaria y social, pública y privada, o la ejecución de un contrato de seguro del que el afectado sea parte.

51) Data Protection Act 2018
Processing of special categories of personal data for insurance and pension purposes
50. Subject to suitable and specific measures being taken to safeguard the fundamental rights and freedoms of data subjects, the processing of data concerning health shall be lawful where the processing is necessary and proportionate for the purposes of the following:
(a) a policy of insurance or life assurance,
(b) a policy of health insurance or health-related insurance,
(c) an occupational pension, a retirement annuity contract or any other pension arrangement, or
(d) the mortgaging of property

52) Data Protection Act (1050/2018) Section 6 Processing of special categories of personal data Article 9(1) of the Data Protection Regulation does not apply:

한편 정보주체의 동의없이 GDPR 제9조 제2항에서 정한 어느 하나에 해당하는 경우에는 건강 정보를 처리할 수 있도록 하고 있는데 이를 따르는 입법례도 있다. 회원국에 따라서는 보험회사의 건강 정보 취급이 동의 취득 이외의 GDPR 제9조 제2항의 요건을 갖추면 정보주체의 동의를 얻지 않고 보험회사가 건강정보를 취급하는 것을 허용하고 있다. 예컨대 영국의 데이터보호법에서는 일정한 조건을 충족했을 경우에 한해 보험에 의한 건강 데이터 취급을 GDPR 제9조 제2항(g) 실질적인 공공의 이익에 필요한 경우에 해당하는 것으로서 보험에서의 건강 데이터 취급을 인정하고 있다.[53]

정보주체의 동의 이외에는 유효한 법적 근거가 없는 것으로 규정하고 있는 입법례를 취하는 경우 각 회원국은 보험회사의 건강데이터 취급시 동의 취득 이외에는 유효한 법적 근거를 인정하지 않고, 계약 전 건강데이터 취득시 및 계약이행시 각각 정보주체의 동의가 있어야 한다. 특히 프랑스의 경우가 이에 해당하는데, 프랑스에서는 보험회사가 건강데이터 취급에 있어 CNIL이 요구하는 건강 정보의 기밀성을 확보하는 규칙을 준수할 필요가 있다.[54][55]

이와 같이 EU 회원국에서는 보험산업에서 건강정보의 취급에 관한 법적 근거는 법규정을 통한 명확화 내지 엄격한 동의요건의 유지 등 다양한 형태로 전개되고 있는데 우리나라의 경우 향후 헬스케어 산업[56]의 발전과 보험자의 역할을

1) when an insurance institution processes data it has received in the course of insurance activities on an insured person's or claimant's state of health, illness or disability, or such data on the treatment or other comparable measures directed at the insured or the claimant that are necessary for determining the liability of the insurance institution;

53) Data Protection Act 2018 제8조 Lawfulness of processing: public interest etc
In Article 6(1) of the GDPR (lawfulness of processing), the reference in point (e) to processing of personal data that is necessary for the performance of a task carried out in the public interest or in the exercise of the controller's official authority includes processing of personal data that is necessary for—
(a)the administration of justice,
(b)the exercise of a function of either House of Parliament,
(c)the exercise of a function conferred on a person by an enactment or rule of law,
(d)the exercise of a function of the Crown, a Minister of the Crown or a government department, or
(e)an activity that supports or promotes democratic engagement.

54) CNIL, Rapport d'activité 2018 Protéger les données personnelles, Accompagner l'innovation, Préserver les libertés individuelles, 2019. 4.

55) 포르투갈에서는 보험 분야의 특별한 개인정보취급에 대해 명확한 규정이 없다. 다만, 법적으로 가입이 의무화되어 있는 보험에 대해서는 GDPR 제9조 제2항(g) '실질적인 공공의 이익에 필요'한 것으로서 보험에서의 건강 데이터 취급을 인정하고 있다.

고려하여 이에 대한 명확한 법체계를 구축할 필요가 있다고 본다.

향후 우리나라가 헬스케어 산업을 육성하고 보험자가 이에 기여할 수 있도록 하기 위해서는 건강정보의 취급은 중요한 과제이다. 이를 위해 현행 개인정보보호법상 건강정보의 처리에 관한 일반규정을 두는 방안을 통해 그 활용에 관한 법적 근거와 한계를 명확히 하는 것이 필요하다고 주장하는 견해가 있다.[57] 이는 타당한 지적으로 여겨지고 정보보호와 관련한 일반법에서 민감한 정보인 건강정보에 대하여 보험산업에서 건강정보의 활용에 관한 법적 근거와 한계를 명확히 법규정화 함으로써 수범자에게는 법적 안정성을 제고할 수 있다고 본다. 또한 다른 대안으로는 개인정보보호법상 법적 근거를 두고 상세한 내용을 자율규제에 맡기는 것도 방법이 될 수 있다. 이러한 경우에는 개인정보보호법 제23조 제1항 제2호에서 말하는 법령의 범위에서만 민감정보의 처리를 가능하도록 하는 법적 근거를 둘 수 있도록 하고 있는데, 이를 법령의 범위로 한정하게 되면 법개정의 어려움이 따르고 보험업계의 현실을 시의적절히 반영하기에 부족하다는 문제가 있을 수 있다. 또한 개인정보보호법 제13조(자율규제의 촉진 및 지원)에 따르면 정보보호위원회는 개인정보처리자의 자율적인 개인정보 보호활동을 촉진하고 지원하기 위하여 개인정보처리자의 자율적인 규약의 제정·시행 지원(동조 제4호)하도록 하고 있다. 이를 체계적으로 해석하면 정보보호위원회가 민감정보에 해당하는 건강정보에 대하여도 자율규제를 통해 활용될 수 있도록 지원할 수 있는지에 대하여 자율규제의 촉진 및 지원이라고 하는 측면에서 보면 가능한 것으로 해석할 여지가 있다. 다만 민감정보에 대하여는 개인정보보호법 제23조가 적용되므로 법령의 범위내에서 민감정보의 처리가 가능한 것처럼 제한적으로 해석될 여지가 있는 점에서 보면 개인정보보호법 제13조가 개인정보처리자의 자율적인 개인정보 보호활동에 관한 규정에도 불구하고 보험업에 있어 민감정보를 활용하기 위한 자율규제의 제정에 관한 법적 근거로서 불분명하게 될 여지가 있다. 따라서

56) 국외 주요 보험사 헬스케어·빅데이터 활용 사례(아시아경제신문 헬스케어·빅데이터 키우는 글로벌 보험사…韓, 역차별 규제에 '한숨'(종합) 2020.07.10. https://www.asiae.co.kr/article/2020071014120458300 내용을 외국보험사 위주로 재구성)

보험사	내용
영국 AIG	생명보험 가입자 대상 원격 의료상담 후 개인 처방전·의약품 배송 서비스 시작
미국 빔	스마트칫솔로 치아관리 데이터를 분석해 치과보험료 산정에 활용
일본 라인	온라인 채팅·메세지 활용해 의사와 의료·건강을 상담하는 유료 원격건강의료상담 서비스

57) 김영국, 앞의 글(개정 데이터 3법과 보험업의 과제), 509면.

해당 조문 즉 23조를 개정하여 법령 및 각종 협회가 금융감독원의 승인 아래 개인정보보호법상 개인정보를 보호하기 위한 자율규제를 제정할 수 있다는 명시적인 규정을 두고, 금융감독원과 협회가 제정한 자율규제가 개인정보보호법의 일반적인 취지에 부합하는지를 심사하도록 하는 규정을 둘 것을 제안한다. 이러한 규정을 통해 보험업과 같이 고객의 개인정보취급이 필수적이고 특수한 경우에 해당하는 업종에서 개인정보를 취급하도록 하고, 보호하는데 산업의 특성을 반영한 명확한 기준을 제시할 수 있을 것으로 생각된다.[58] 앞서 살펴본 바와 같이 독일 보험업 정보보호행동강령 제6조는 건강정보가 활용될 수 있는 경우에 대하여 상세하게 규정하고 있음을 보았다. 우리의 경우에도 협회차원에서 보험자로부터 건강정보와 같은 민감한 정보를 향후 새로운 상품을 개발함에 있어 보험자가 어떠한 형태로든 활용하기 위해 꼭 필요한 내용에 대한 의견을 수렴하여 자율규제에 반영한다면 건강정보의 활용에 대한 일반규정화 보다도 보험업의 특수성을 더욱 반영하여 건강정보의 적극적인 활용이 가능한 환경을 정비할 수 있을 것으로 기대된다.

58) 이와는 달리 보험업감독규정을 통해 개인정보 활용에 관한 명시적인 규정을 둘 것을 제안하는 견해도 있다; 김경환, 강민규, 이해랑, 「보험개인정보 보호법제 개선방안」, 보험연구원, 2014, 151면 (이 견해에 의하면 보험업에 있어 건강정보의 취급에 대해 보험업감독규정에 법적 근거를 두면 강제력을 부여할 뿐만 아니라, 준수에 따른 책임성을 명확히 하여 실무자들이 믿고 따를 수 있게 하는 장점이 있을 수 있다. 나아가 개인정보를 규율하는 일반법으로 개인정보보호법이 존재하고 있는 점을 고려하여 보험업에 적합한 개인정보처리에 관한 지침을 제정하는 경우에는 단순한 보충성의 원칙을 따를 것이 아니라 보험업의 특성을 반영하여 차별성을 부여하여 실용성을 제고할 필요가 있다고 한다). 해당 견해는 개인정보의 보호와 활용에 관한 법적 강제력의 강화라고 하는 측면에서 보면 일견 타당성이 있는 주장이라고 보이나, 보험업감독규정 제1조에서 명시하고 있는 바와 같이 행정규칙에 해당하는 보험업감독규정은 보험업법, 보험업법시행령, 보험업법시행규칙, 금융위원회의 설치 등에 관한 법률, 금융위원회의 설치 등에 관한 법률 시행령, 외국환거래법, 외국환거래법시행령 그 밖의 관련법령으로 "보험관련법령"에서 금융위원회에 위임한 사항과 그 시행에 필요한 사항을 정함을 목적으로 제정된 것으로 개인정보보호법을 보험관련법령이라고 일반적으로 해석할 수 있는지 의문이며, 감독당국인 금융위원회에 위임한 사항과 그 시행에 필요한 사항을 정하는 것이 동 행정규칙의 주된 제정목적임에 비추어 개인정보를 취급하는 업무를 하는 보험회사에 대하여 개인정보보호위원회의 위임사항이 있을 수 있는데 이를 성질이 다른 보험업감독규정에 규정하는 것은 법체계상 부적합한 것으로 생각된다.

Ⅴ. 나가며

최근 개인정보에 대한 관심이 높아지고 있다. 개인정보는 '21세기의 석유'라 칭해지듯이 혁신의 촉진에 이바지하는 이용가치가 높은 자원으로 파악되고 있다.

개인정보의 수집·분석에 의해 소비자 개개인의 행동이나 경향을 보다 적확하게 파악·예측할 수 있어 지금까지 없었던 획기적인 제품·서비스의 개발, 여러 가지 사회적 과제의 해결 등이 기대되고 있다. 보험업도 예외는 아니어서 고객의 개인정보를 활용한 새로운 보험상품의 개발이 기대되고 고객 맞춤형 보험상품을 설계할 수 있는 기회가 된다. 다만 어디까지나 고객의 개인정보는 활용의 대상이면서 동시에 보호의 대상이 되고 있으므로 정보주체의 정보주권의 강화에 따른 관련 법제의 변화는 불가피한 상황이다. 이러한 상황을 대변하듯 앞서 살펴본 바와 같이 보험업에서 개인정보의 활용과 관련하여 EU GDPR 시행 후 보험업계가 당면한 과제는 우리에게 상당한 시사점을 주고 있다. 독일의 경우 GDPR 시행 후 자율규제에 해당하는 보험협회 차원에서 정보보호행동강령을 제정하여 보험업에서 고객정보의 활용과 보호에 관한 일정한 기준을 제시하고 있다. 해당 행동지침의 내용은 EU GDPR의 내용을 대부분 수용하면서도 보험업의 특성을 반영하고 있다는데 그 의의가 있다. 앞서 논한 바와 같이 이러한 자율규제형식의 행동지침을 우리나라의 경우에도 협회차원에서 도입하여 개정 개인정보보호법 체계에서 고객의 개인정보의 활용과 보호에 관한 명확한 기준을 제시할 필요가 있다고 본다. 이 외에도 보험업의 디지털화에 따라 고객의 개인정보의 활용을 위한 법체계를 구축하되, 정보주체의 정보주권을 강화하는 정보주체의 권리를 GDPR을 참고로 적극적으로 도입할 필요가 있다고 본다. 이러한 입법적인 노력은 결국 보험업에 있어 개인정보의 활용과 보호 양자의 가치를 모두 고려하고자 하는 국제적인 입법추세에 부합하는 것이라고 생각된다.

참고문헌

김경환, 강민규, 이해랑, 「보험개인정보 보호법제 개선방안」, 보험연구원, 2014.

김영국, "헬스케어서비스 활성화를 위한 법정책 과제-빅데이터에 기반한 개인의료정보의 활용을 중심으로-", 「보험법연구」 제13권 제2호, 한국보험법학회 2019.
- "개정 데이터 3법과 보험업의 과제-디지털 헬스케어서비스 활성화를 중심으로-, 「보험법연구」제14권 제1호, 한국보험법학회, 2020.

이희옥, "빅테이터 환경에서 보험업상 개인정보의 보호와 활용", 「소비자문제연구(제50권 제2호)」, 한국소비자원, 2019. 8.

최창희/홍민지, 「빅데이터 활용 현황과 개선 방안」, 보험연구원, 2019.

황현아, 마이데이터 산업의 내용과 과제: 신용정보법 개정안을 중심으로, KiRi 리포트 2019. 4. 22.

access now, ONE YEAR UNDER THE EU GDPR AN IMPLEMENTATION PROGRESS REPORT, 2019.

Brandi, Schutz von Gesundheitsdaten, Informationen zum Datenschutz I Februar 2020, S. 2(https://mail.google.com/mail/u/0/?tab=rm&ogbl#inbox/FMfcgxwJXLfqFfFsjfWWzpvzxjKBgNfl?projector=1&messagePartId=0.1).

European Commission, MULTISTAKEHOLDER EXPERT GROUP TO THE STOCK-TAKING EXERCISE OF JUNE 2019 ON ONE YEAR OF GDPR APPLICATION Multistakeholder Expert Group to support the application of Regulation (EU) 2016/679 Report 13. 7. 2019.

Gregory Voss, After Google Spain and Charlie Hebdo: The Con-tinuing Evolution of European Union Data Privacy Law in a Time of Change,71BUS.LAW. 281, 283–84 (2015).

KPMG, "The GDPR and key challenges faced by the Insurance industry" 2018. 2.

Martin et al. (2018): Das Sanktionsregime der Datenschutz-Grundverordnung: Auswirkungen auf Unternehmen und Datenschutzaufsichtsbehörden. Hrsg.: Michael Friedewald et al., Forum Privatheit und selbstbestimmtes Leben in der digitalen Welt, Karlsruhe: Fraunhofer ISI. 2019.

Monica A. Senor, Massimo Durante, REPORT ON THE HARMONIZATION OF ITALIAN LAW WITH THE ENFORCEMENT OF THE EU GENERAL DATA PROTECTION REGULATION 2016/679(https://blogdroiteuropeen.files.wordpress.com/2018/06/italy.pdf).

SMEunited "Multi-stakeholder expert group to support the application of Regulation (EU) 2016/679 SMEunited1 input to the QUESTIONS TO PREPARE THE STOCK-TAKING EXERCISE OF JUNE 2019 ON THE APPLICATION OF GDPR" (2019.4).

Sonia Cisse, France - National GDPR Implementation Overview(https://www.dataguidance.com /notes/france-national-gdpr-implementation-overview).

2019년 1월 7일자 보험신보 기사 참조(insweek.co.kr/45760).

〈Zusammenfassung〉

Rechtliche Fragen der Nutzung und des Schutzes personenbezogener Daten nach der Digitalisierung der Versicherungswirtschaft

- Mit Schwerpunkt auf dem Vergleich des EU-DSGVO und des Datenschutzkodex der Versicherungswirtschaft in Deutschland -

Ji, Gwang Woon*

Die Versicherungswirtschaft ist von jeher darauf angewiesen, in großem Umfang personenbezogene Daten der Versicherten zu verwenden. Sie werden zur Antrags-, Vertrags-, und Leistungsabwicklung erhoben, verarbeitet und genutzt, un Versicherte zu beraten und zu betreuen sowie um das zu versichernde Risiko einzuschätzen, die Leistungspflicht zu prüfen und Versicherungsmissbrauch im Interesse der Versichertengemeinschaft zu verhindern. Versicheurngen können dabei heute ihre Aufgaben nur noch mit Hilfe der elektronischen Datenverarbeitung erfüllen.

Die Wahrung der informationellen Selbstbestimmung und der Schutz der Privatsphäre sowie die Sicherheit der Datenverarbeitung sind für die Versicherungswirschaft ein Kernanliegen, um das Vertrauen der Versicherten zu gewährleisten. Die Versicherungsunternehmen müssen die gesetzleichen Regelungen zur Verarbeitung personbezogener Daten nachkommen. Darüber hinaus haben sie nicht nur im Einklang mit den Bestimmungen des Datenschutgesetzes, sondern auch die Erfüllung der Verpflichtung von beigetretennen Unternehmen der Versicherungswirtschaft, den Grundsätzen der Transparenz und die Erforderlichkeit der verarbeiteten Daten und die Datenminimierung in besonderer Weise nachzukommen.

In diesem Zusammenhang untersucht der vorliegende Beitrag die

* Lecturer at Chungbuk National University, Dr.Jur & Ph.D in Law.

rechtlichen Fragen im Zusammenhang mit der Richtung der Nutzung, der Verwendung und des Schutzes von Kundensdaten, die sich ergeben können, wenn die Digitalisierung des Versicherungsgeschäfts im Bewusstsein der oben genannten Probleme fortgesetzt wird. Dabei wird die 2018 in Kraft getretene Europäische Allgemeine Datenschutzverordnung (DSGVO) vergleichend betrachtet. Datenschutz und -nutzung unter der Berücksichtigung der Erkenntnis, dass es wichtig ist, ein angemessenes Gleichgewicht zwischen dem Schutz der persönlichen Daten und der Nutzung und Verwendung des Betreibers zu gewährleisten, um durch diese Regelung die Sicherheit der Datenhoheit des Betroffenen zu stärken und persönliche Daten effektiv zu nutzen. Im folgenden werden im Bewußtsein dieser Problematik die wichtigsten Regelungen des DSGVO vorgestellt, die in Bezug auf die Versicherungswirtschaft als wichtig anerkannt werden, was die Versicherungswirtschaft nach der Umsetzung als Aufgabe anerkennt, sowie die für die Versicherungswirtschaft in Deutschland geltenden Datenschutz-Verhaltensrichtlinien (Datenschutzkodex). Mit dieser rechtvergleichenden Betrachtung wird es eindeutig, dass die Umgang und Regelung mit den personbezogenen Daten der Versicherten im betreffenen Gesetze für das persönsiche Datenschutz in Korea aufgestellt werden sollen.

Key Words : Datenschutzgesetz, Massendaten, Die Datenschutz-Grun dverordnung, Betroffene, Selbstverwaltung