

## ■ Legal Update ■

## EU 개인정보보호규정 시행 관련 러시아 내 개인정보 처리 유의사항

지평 러시아 · 중앙아시아팀

### 1. EU 개인정보보호규정 시행

2018년 5월 25일부터 EU의 개인정보보호규정, General Data Protection Regulation (GDPR) No. 2016/679<sup>1</sup>이 시행 예정입니다. EU 내에 사업장을 가진 기업뿐 아니라 EU 내 거주자와 거래하는 기업에 대해서도 규정이 적용되므로 러시아에 설립된 한국 기업(러시아 법인)도 그 적용대상이 될 수 있습니다. 위반 시 처벌의 규모가 상당하기 때문에 이에 대한 대비가 필요할 것으로 판단됩니다. EU의 개인정보보호규정의 주요 내용과 함께 개인정보보호에 관한 러시아연방법률의 주요 내용을 정리하였습니다.

### 2. EU 개인정보보호규정(GDPR) 주요 내용

#### 가. 개요

General Data Protection Regulation (GDPR) No. 2016/679 (이하 '본 개인정보보호규정')는 유럽 연합(EU) 시민들의 개인정보보호를 강화하기 위해 유럽의회에서 제정한 통합 규정으로, 2016년 공표된 후 약 2년간의 유예 기간을 거쳤으며 2018년 5월 25일 시행 예정입니다.

<sup>1</sup> <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN>

기업이 EU 시민의 개인정보가 포함된 데이터를 활용하는 경우 본 개인정보보호규정을 준수해야 하며, 그 주요 내용으로는 ① 정보제공자로부터의 개인정보처리에 관한 명확한 사전동의 ② 정보제공자의 개인정보에 대한 통제권 강화 ③ 기업 내 개인정보처리 절차 강화 ④ 정보의 역외이전 절차 규정 등이 포함됩니다.

## 나. 주요 내용

### 1) 적용대상

EU 내에 사업장을 두고 EU 역내 정보주체(이하 '정보제공자')의 개인정보를 처리, 활용하는 기업 및 EU 내에 사업장은 없으나 EU 거주자에게 재화나 서비스를 제공하거나 EU 거주자의 EU 내 행동을 모니터링하는 기업에게 적용됩니다. 따라서 해당 기업이 EU 내에 사업장을 두고 있는지 여부에 관계없이 기업의 거래 상대방이 EU 역내에 거주하고 있는 경우에 적용대상이 됩니다.

나아가, 역내 정보제공자는 EU 시민으로 한정되지 않으며, 지리적으로 EU 내에 위치한 정보제공자의 경우 국적과 관계없이 본 개인정보보호규정에 따라 보호되는 정보제공자에 해당됩니다. 따라서, EU 역내에 거주하는 한국 및 또는 러시아 시민(소비자)에게 재화 및 서비스를 공급하는 러시아 법인의 경우 해당 소비자의 개인정보를 저장, 처리하는 경우 본 개인정보보호규정의 적용대상이 됩니다.

### 2) 적용대상이 되는 개인정보의 범위

① 이름, 주소, ID 등 기본 신상정보 ② 위치 IP주소, 쿠키, 데이터, RFID 태그 등 웹 정보 ③ 건강, 유전정보 ④ 생체, 인종, 민족 정보 등 특정개인을 식별할 수 있는 정보는 '개인정보'에 해당됩니다.

### 3) 개인정보처리에 관한 사전동의

본 개인정보보호처리규정에 따라 기업은 정보제공자의 명확한 동의(explicit consent)를 취득한 경우에 한하여 개인정보를 처리할 수 있습니다. 동의서에는 정보를 수집하는 기업과 관련 파트너사에 관한 구체적이고 명확한 정보가 포함되어야 하며, 개인 정보 수집의 목적이 고지되어야 합니다. 암묵적인 동의는 동의로 간주되지 않으며 정보제공자는 진술이나 적극적인 행동(by clear affirmative action)을 통해 동의 의사를 표시해야 합니다. 반드시 사전동의를 취득해야 합니다.

### 4) 정보제공자의 개인정보에 대한 통제권 강화

정보를 제공한 정보제공자는 언제든지 본인이 제공한 정보에 대한 동의를 철회할 수 있으며, 개인정보처리자에 대하여 인터넷상에서 자신의 개인 정보를 삭제해 줄 것을 요청할 수 있습니다. 다만, 공공보건분야 또는 통계, 역사적, 과학적 연구목적으로 정보가 필요한 경우에는 삭제권의 행사를 거부할 수 있습니다.

정보제공자는 정보처리자인 기업에 대하여 개인정보열람 및 개인정보처리 현황을 요청할 수 있습니다. 정보제공자가 본인의 개인정보처리 현황을 요청하는 경우, 해당 기업은 요청받은 날로부터 1개월 이내에 관련 정보를 제공해야 합니다.

정보제공자는 기업이 보관하고 있는 자신의 개인정보를 제3자에게 이전해 줄 것을 요구할 권리(right to data portability)를 가집니다. 그 외에 정보제공자의 변경권, 처리제한권, 거부권, 자동화된 결정 및 프로파일링 관련 통제권 등이 보장됩니다.

### 5) 기업 내 개인정보처리 절차 강화

본 개인정보보호규정에 따르면, ① 정보를 수집, 처리하는 회사가 공공기관인 경우 ② 민감한 정보를 다루는 경우 ③ 대중의 성향과 행동을 모니터링하는 경우 해당 기업은 반드시 데이터보호관리자(Data Protection Officers: 이하 DPO)를 임명해야 합니다. DPO는 회사 내부 또는 외부에서 개인정보보호규정의 준수여부를 확인하고 자문하며 권고사항을 제시하는 직책으로, 사내에 기존 직원 중에 임명하거나 외부 전문가와의 계약을 통해 업무를 수행하도록 할 수도 있습니다.

나아가 직원 수가 250명 이상인 기업은 개인정보처리 활동을 반드시 문서화해야 합니다. 또한 직원 수가 250명 이하라 하더라도 처리하는 개인정보가 정보제공자의 권리를 침해할 수 있는 경우 이를 문서화해야 하며, 특히, 종교, 사상 등 민감한 개인정보 및 범죄 관련 개인정보를 처리하는 경우에는 직원의 수와 관계없이 모든 처리활동을 기록해야 합니다. 문서화된 기록에는 정보처리 주체, 목적, 범위, 제3국으로 이동 시 해당 국가명, 정보 말소기한 등의 정보를 명시해야 합니다.

개인정보가 유출되는 경우에는 해당국 감독기관으로 72시간 이내에 보고해야 하며, 이로 인하여 정보제공자의 권리를 침해하는 중대한 문제가 발생할 가능성이 있는 경우 지체없이 정보제공자에게 통지해야 합니다.

## 6) 개인정보의 역외이전 규정

EU 역내에서 수집된 개인정보의 역외이전은 해당 국가가 EU에 상응하는 수준의 정보보호체계를 갖추고 있으며, 안전한 개인정보보호수준을 보장하는 경우에 한하여 가능합니다. 따라서, EU의 개인정보보호 적정성 평가 승인 국가의 한하여 개인정보의 역외이전이 가능하며, 그 밖에 승인을 받지 못한 국가의 기업의 경우 EU 행동강령, 기업규칙 준수를 통해 개인정보가 안전하게 보호되고 있다는 사실을 증명하는 경우에 한하여 역외이전을 할 수 있습니다. 현재 한국은 EU 적정성 평가 절차를 거치는 중에 있으나, 아직은 승인을 받지 못하였으므로 개인정보의 역외이동 시 규정 준수를 위한 조치가 필요합니다.

## 7) 처벌규정

본 개인정보보호규정을 위반하는 기업에 대해서는 사안의 경중에 따라 최대 2,000만 유로 또는 전 세계 매출액의 4% 중 더 높은 금액을 과징금으로 부과합니다.

## 3. 개인정보보호에 관한 러시아연방법률에 따른 개인정보의 현지화 규정

### 가. 개요

개인정보보호에 관한 러시아연방법률(이하 '개인정보보호법') 제18조 제5항(이하 '본 조항')에 따르면, 개인정보처리자가 온라인 또는 오프라인으로 러시아 국민의 개인정보를 수집한 때에는, 해당 개인정보를 반드시 러시아연방 영토 내의 서버에 기록, 시스템화, 축적, 저장, 업데이트, 변경할 의무가 있습니다.

### 나. 주요 내용

#### 1) 적용대상

개인정보보호법에 따르면, '개인정보'란, 다른 사람으로부터 개인을 식별할 수 있는 모든 직접적, 간접적 정보를 포함한다고 하여 상당히 넓은 개념으로 정의되고 있습니다. 또한 '개인정보의 수집'은 개인정보처리자가 정보제공자의 개인정보를 정보제공자로부터 수집을 목적으로 하여 직접적으로 전달받는 것을 의미합니다. 나아가 '개인정보처리자'란, 업무를 목적으로 개인정보파일을 운용하기 위하여 스스로 또는 다른 사람을 통하여 개인정보를 처리하는 공공기관, 법인, 단체, 개인 등을 포함합니다. 따라서, 러시아 내에서 영업활동을 하는 기업(러시아 법인)이 러시아 국민의 개인정보를 수집, 전달, 저장하는 경우에는 개인정보보호법의 적용대상이 됩니다.

## 2) 개인정보의 현지화 원칙

러시아연방 통신부는 개인정보처리자가 러시아 내의 데이터베이스를 기본 데이터베이스(primary database)로 하여 러시아 국민의 개인정보를 보관한 경우에는, 그 기본 데이터베이스에 보관된 정보에 한하여 사본의 형태로 해외의 데이터베이스(secondary database)에 보관하는 것이 가능하다고 유권해석을 내린 바 있습니다. 다시 말해, 러시아 내에서 수집된 러시아 국민의 개인정보는 우선적으로 러시아 내에 보관하는 것이 원칙이며, 그 이후에 이를 해외로 이전하여 보관하는 것은 허용된다는 해석입니다.

개인정보보호법은 “데이터베이스”에 대해 명확한 정의를 내리고 있지 않으나, 본 조항의 문언상 데이터베이스란 (i) 출력한 문서를 보관하는 파일, (ii) 전자문서가 보관된 컴퓨터파일, (iii) 전자서버를 모두 포함하는 넓은 개념으로 해석됩니다. 따라서 그 형식을 불문하고 보관/저장된 내용이 개인정보에 해당하는 경우에는 개인정보보호법에서 규제하는 데이터베이스로 해석되므로 출력된 문서(하드카피)의 경우에도 반드시 그 원본은 러시아 내에 보관하는 등 본 조항의 규정을 준수할 필요가 있습니다.

## 3) 개인정보의 국가 간 이전 요건

개인정보보호법 제12조 제1항 및 제2항에 따르면 개인정보를 이전하고자 하는 국가가 개인정보자 동치리에 관한 개인정보보호에 관한 유럽협약(Council of Europe Convention on the Protection of Individuals with Regard to Automatic Processing of Personal Data)의 가입국이거나 또는 러시아 정부에 의해서 개인정보보호의 수준이 안전하다고 승인된 국가의 경우에는 정보제공자의 서면 동의 없이도 개인정보의 국가 간 이전이 가능합니다. 그러나 그 외의 국가로 이전하는 때에는 반드시 정보제공자의 서면동의가 필요합니다(제4항).

2013년 3월 15일 자 러시아연방 통신언론부령 No.274(최근 개정 2017.06.15.)에 따르면, 대한민국은 러시아 정부에 의해 개인정보보호의 수준이 안전한 것으로 승인된 국가에 해당됩니다. 따라서 개인정보 현지화 요건을 갖춘 경우 정보제공자의 서면동의가 없어도 한국 본사로의 개인정보의 이동이 가능합니다. 그러나 동 부령에 미국, 중국, 일본 등은 이에 포함되지 않으므로 미국 등으로 개인정보를 이동하는 경우에는 반드시 정보제공자의 서면동의가 필요합니다.

#### 4) 처벌규정

본 조항을 위반하는 경우 행정위반에 관한 러시아연방법률 제13.11조에 따라, 10,000루블(약 \$175)의 벌금이 부과될 수 있습니다.

#### 4. 결론 및 시사점

EU의 개인정보보호규정은 EU 내 거주자와 거래하는 외국 기업에 대해서도 적용되므로 러시아 소재 한국 기업(러시아 법인)도 그 적용대상이 됩니다. 위반 시 처벌의 규모가 상당하므로 EU 내 소비자와 거래하는 경우 개인정보보호규정에서 요구하는 사내시스템을 구축하는 등 주의를 기울여야 할 것으로 판단됩니다.

나아가 러시아 소재 한국 기업(러시아 법인)이 러시아 직원을 포함한 러시아 국민의 개인정보를 수집, 보관하는 때에는 개인정보보호에 관한 러시아연방법률이 정한 바에 따라 러시아 국민의 개인정보 현지화 요건을 갖추어야 하며 개인정보의 국가 간 이동 시 정보제공자의 사전동의를 취득하여야 하므로, 개인정보 처리과정에서 러시아 법률이 정한 절차 및 요건 준수 여부에 관한 면밀한 검토가 필요할 것입니다.

※ 참고자료 : 한국인터넷진흥원(KISA) “우리기업을 위한 GDPR 안내서”

위 내용에 대한 문의 또는 러시아 · 중앙아시아팀 사건 문의는 아래 담당 변호사에게 연락해주시기 바랍니다.

[담당 변호사]

러시아 모스크바 사무소	<p>이승민 선임외국변호사(러시아) · 모스크바 사무소장                  Tel. +7-495-795-3268 Email. smlee@jipyong.com</p>
본사 러시아 · 중앙아시아팀	<p>류혜정 파트너변호사 · 본사 팀장                  Tel. 02-6200-1722 Email. hjryu@jipyong.com</p>