『유럽연합, 데이터 프라이버시 프레임워크』 심층분석 보고서

2023. 8.

통보문서 번호	미통보문	규제분야	정보디지털
통보국	유럽연합	HS Code	-
작성기관	TBT종합지원센터	작성자 문의처	박형준 02-3487-7754

국가기술표준원
Korean Agency for Technology and Standards

KOTICA
한국시험연중산업협회

[목 차]

1 규제 개요

□ 발표 내용

○ '23.7.10., EU 집행위원회는 EU-U.S. DPF*에 대한 적합성 결정을 채택함

- 미국은 새로운 프레임워크에 따라 EU에서 미국 기업으로 전송되는 개인 데이터에 대해 유럽연합과 유사한 수준의 보호를 보장함
- 새로운 적합성 결정에 따라 개인 데이터는 추가적인 데이터 보호 장치를 마련하지 않고도 EU에서 프레임워크에 참여하는 미국 기업으로 안전하게 전송할 수 있음
- 프레임워크는 미 상무부에서 관리 및 모니터링하며, 미국 연방 무역 위원회는 미국 기업의 규정 준수를 강제할 예정[1)]

* DPF란 데이터 프라이버시 프레임워크(Data Privacy Framework)를 말함

규제명	▪ EU-미국 데이터 프라이버시 프레임워크에 따른 적절한 수준의 개인 데이터 보호, 결정, 2023년 7월 ▪ Adequate Level of Protection of Personal Data under the EU-US Data Privacy Framework, Decision, July 2023
규제부처	▪ EU Commission, U.S. Department of Commerce ▪ EU 위원회, 미국 상무부
요구사항 유형	▪ 데이터 보호
제·개정 상태	▪ 제정 채택안
WTO TBT 통보	▪ 미통보문
고시일	▪ 2023년 7월 10일
채택일	▪ 2023년 7월 10일
의견수렴 마감일	▪ -
발효일	▪ -
준수 기한	▪ -

□ 적용범위 및 수출규모

적용대상	▪ 데이터 ▪ Data
HS Code	▪ 제품이 아닌 데이터 보호에 관한 규정으로 HS Code 특정이 어려움
對발행국 수출액 (천불)	▪ -

1) https://ec.europa.eu/commission/presscorner/detail/en/ip_23_3721

2 규제 제·개정 내용

□ (제 1조) 목적

○ 미국은 부속서 1*의 섹션 1.3에 따라 미국 상무부가 유지 및 관리하고 공개적으로 제공하는 '데이터 프라이버시 프레임워크 목록'에 포함된 EU에서 미국 내로 전송되는 개인 데이터에 대해 적절한 수준의 보호를 보장해야 함

* 부속서 1. EU-U.S. 데이터 프라이버시 프레임워크 원칙

□ (제 2조) 회원국 고지

○ 회원국의 관할 당국이 개인 데이터 처리와 관련하여 개인을 보호하기 위해 제1조에서 언급된 데이터 전송과 관련하여 (EU) 2016/679 제58조에 따른 권한을 행사하는 경우, 해당 회원국은 위원회에 이를 통보해야 함

□ (제 3조) 주요 의무사항

1	- 위원회는 미국이 제1조에서 언급한 적절한 수준의 보호를 지속적으로 보장하고 있는지 평가하기 위해 이전된 데이터에 접근할 수 있는 조건을 포함하여 본 결정의 대상인 법적 프레임워크의 적용을 모니터링해야 함
2	- 회원국과 위원회는 부속서 1에 명시된 원칙의 준수를 강제할 수 있는 법적 권한을 가진 미국 내 조직이 부속서 1에 명시된 원칙의 위반을 확인하고 처벌할 수 있는 효과적인 탐지 및 감독 메커니즘을 제공하지 않는 것으로 보이는 경우 서로에게 알려야 함
3	- 회원국과 위원회는 국가 안보, 법 집행 또는 기타 공익을 추구할 책임이 있는 미국 공공 기관이 개인 데이터 보호에 대한 개인의 권리에 대한 간섭이 필요하고 비례적인 수준을 넘어서거나 그러한 간섭에 대한 효과적인 법적 보호가 없다는 징후가 있는 경우 서로에게 알려야 함
4	- 본 결정이 회원국에 고지된 날로부터 1년 후, 위원회 및 유럽 데이터 보호 위원회와 긴밀히 협의하여 결정되는 시기에 위원회는 미국의 관할 조직과 함께 수행한 검토를 통해 얻은 정보를 포함하여 이용 가능한 모든 정보를 기반으로 결과를 평가해야 함
5	- 위원회가 적절한 수준의 보호가 더 이상 보장되지 않는다는 징후가 있는 경우, 위원회는 이를 관할 미국 당국에 통보해야 함 - 필요한 경우, 위원회는 본 결정을 일시 중단, 수정 및 폐지하거나 그 범위를 제한하기로 결정해야 함 - 위원회는 미국 정부의 협조 부족으로 인해 미국이 적절한 수준의 보호를 계속 보장하고 있는지 여부를 판단할 수 없는 경우 이러한 결정을 채택할 수 있음

□ 부속서 1. 미국 상무부가 발표한 EU-U.S. 데이터 프라이버시 프레임워크 원칙

ㅇ (고지)

a	- 조직은 개인에게 다음 사항을 알려야 함 I. EU-U.S. DPF에 참여하고 있으며 데이터 프라이버시 프레임워크 목록에 대한 링크 또는 웹 주소를 제공해야 함 ii. 수집된 개인 데이터 유형 및 해당되는 경우 원칙을 준수하는 조직의 미국 법인 또는 자회사 iii. EU-U.S. DPF에 의거하여 EU로부터 받은 모든 개인 데이터에 대해 원칙에 따르겠다는 약속 iv. 개인 정보를 수집하고 사용하는 목적 v. 문의 및 불만 사항에 대응할 수 있는 EU 내 관련 기관을 포함하여 해당 조직에 연락하는 방법 vi. 개인 정보를 공개하는 제3자의 유형 또는 신원 및 공개 목적 vii. 개인이 자신의 개인 데이터에 접근할 수 있는 권리 viii. 개인 데이터의 사용 및 공개를 제한하기 위해 조직이 개인에게 제공하는 선택 및 수단 ix. 불만 사항을 해결하고 개인에게 무료로 적절한 해결책을 제공하기 위해 지정된 독립적 분쟁 해결 조직 및 해당 조직이 (1)~(3)에 해당하는지 여부 사항 (1) DPA에 의해 설립된 패널 (2) EU에 기반을 둔 대체 분쟁 해결기관 (3) 미국에 기반을 둔 대체 분쟁 해결기관 x. FTC*, DOT** 또는 미국 공인 법정 기관의 조사 및 집행 권한의 적용을 받는 경우 * FTC : 연방통상위원회 ** DOT : 미국 교통부 xi. 특정 조건 하에서 개인이 구속력 있는 중재를 요청할 수 있는 가능성 xii. 국가 안보 또는 법 집행 요건을 충족하는 것을 포함하여 공공 기관의 합법적 요청에 대한 응답으로 개인 정보를 공개해야 하는 경우 xiii. 제3자에게 개인 정보를 이전하는 경우의 책임
b	- 이러한 고지는 개인이 처음 조직에 개인 정보를 제공하도록 요청받았을 때 또는 가능한 한 빨리 제공되어야 함 - 단, 조직이 해당 정보를 이전 조직에서 원래 수집 또는 처리한 목적이 아닌 다른 목적으로 사용하거나 제3자에게 처음으로 공개하기 전에는 어떠한 경우에도 명확하고 눈에 잘 띄는 언어로 제공해야 함

ㅇ (선택)

a	- 조직은 개인에게 자신의 개인 정보가 (i) 제3자에게 공개될지 또는 (ii) 원래 수집된 목적이나 이후 개인이 승인한 목적과 실질적으로 다른 목적으로 사용될지 여부를 선택할 수 있는 기회(즉, 거부할 수 있는 기회)를 제공해야 함

	- 또한, 개인이 선택권을 행사할 수 있도록 명확하고 눈에 잘 띄며 쉽게 이해할 수 있는 매커니즘을 제공해야 함
b	- 예외로, 조직을 대신하여 조직의 지시에 따라 업무를 수행하는 대리인 역할을 하는 제3자에게 공개하는 경우, 선택권을 제공할 필요는 없음 - 단, 조직은 항상 대리인과 계약을 체결해야 함
c	- 민감한 정보*의 경우, 조직은 해당 정보를 (i) 제3자에게 공개하거나 (ii) 원래 수집한 목적 또는 이후 옵트인** 선택권 행사를 통해 개인이 승인한 목적 이외의 용도로 사용하려는 경우 개인으로부터 긍정적인 명시적 동의(옵트인)를 얻어야 함 - 또한, 조직은 제3자로부터 받은 개인 정보를 제3자가 민감한 정보로 식별하고 취급하는 경우, 이를 민감한 정보로 취급해야 함 * 의료 또는 건강 상태, 인종, 민족적 기원, 정치적 의견, 종교, 철학적 신념, 노동조합 가입 여부, 개인의 성생활 등을 명시하는 개인 정보 ** 옵트인(Opt-in)이란 당사자가 개인 데이터 수집을 허용하기 전까지 당사자의 데이터 수집을 금지하는 제도를 뜻함

ㅇ (제3자 이전에 대한 책임)

a	- 컨트롤러(개인정보처리자) 역할을 하는 제3자에게 개인 정보를 이전하려면 조직은 고지 및 선택 원칙(Notice and Choice Principles)을 준수해야 함 - 조직은 제3자 컨트롤러와 계약을 체결해야 하며, 데이터는 개인이 제공한 동의와 일치하는 목적으로만 처리할 수 있음 - 수신자가 원칙과 동일한 수준의 보호를 제공하고 더 이상 이러한 의무를 이행할 수 없다고 판단하는 경우, 조직에 통지해야 함 - 해당 계약에 결정이 내려질 경우, 제3자 컨트롤러가 처리를 중단하거나 합리적이고 적절한 조치를 취하도록 규정해야 함
b	- 대리인 역할을 하는 제3자에게 개인 데이터를 전송하려면 조직은 다음을 수행해야 함 (i) 제한적이고 지정된 목적으로만 해당 데이터를 전송해야 함 (ii) 대리인이 본 원칙에서 요구하는 것과 최소한 동일한 수준의 개인 정보 보호를 제공할 의무가 있는지 확인해야 함 (iii) 대리인이 원칙에 따른 조직의 의무에 부합하는 방식으로 전송된 개인 정보를 효과적으로 처리할 수 있도록 합리적이고 적절한 조치를 취해야 함 (iv) 대리인이 원칙에서 요구하는 것과 동일한 수준의 보호를 제공할 의무를 더 이상 이행할 수 없다고 판단하는 경우 이를 조직에 통지하도록 요구해야 함 (v) (iv)를 포함하여 통지 즉시 무단 처리를 중단하고 시정하기 위한 합리적이고 적절한 조치를 취해야 함 (vi) 요청 시 해당 대리인과의 계약에 포함된 관련 개인 정보 보호 조항의 요약본 또는 대표 사본을 부처*에 제공해야 함 * 부처란 미국 상무부를 의미함

ㅇ (보안)

a	- 개인 정보를 생성, 유지, 사용 또는 배포하는 조직은 개인 정보의 처리에 관련된 위험과 개인 정보의 특성을 적절히 고려하여 개인 정보의 손실, 오용 및 무단 접근, 공개, 변경 및 파기를 방지하기 위한 합리적이고 적절한 조치를 취해야 함

ㅇ (데이터 무결성 및 목적 제한)

a	- 원칙에 따라 개인 정보는 처리 목적과 관련된 정보로 제한되어야 함 - 조직은 개인 정보를 수집한 목적 또는 이후 개인이 승인한 목적과 양립할 수 없는 방법으로 개인 정보를 처리해서는 안됨 - 이러한 목적에 필요한 범위 내에서 조직은 개인 데이터가 의도된 용도에 맞게 신뢰할 수 있고 정확하며 완전하고 최신 상태에서 확인하기 위해 합리적인 조치를 취해야 함 - 조직은 해당 정보를 보유하는 동안 원칙을 준수해야 함
b	- 정보는 (a)의 의미 내에서 처리 목적에 부합하는 경우에만 개인을 식별하거나 식별할 수 있는 형태로 보유할 수 있음 - 이러한 의무는 조직이 공익, 저널리즘, 문학 및 예술, 과학 및 역사 연구 그리고 통계 분석 목적에 합리적으로 부합하는 범위 내에서 개인 정보를 더 오랫동안 처리하는 것을 막지 않음 - 이러한 처리는 EU-U.S. DPF의 다른 원칙 및 조항의 적용을 받아야 함 - 조직은 이 조항을 준수하기 위해 합리적이고 적절한 조치를 취해야 함

ㅇ (정보 열람)

a	- 개인은 조직이 보유한 자신의 개인 정보에 접근할 수 있어야 하며, 해당 정보가 부정확하거나 원칙을 위반하여 처리된 경우 해당 정보를 정정, 수정 또는 삭제할 수 있어야 함 - 단, 접근 권한 제공에 따른 부담이나 비용이 개인 정보에 대한 위험과 불균형하거나 개인 이외의 사람의 권리가 침해되는 경우는 제외함

ㅇ (청구, 집행 및 책임)

a	- 효과적인 개인 정보 보호에는 원칙 준수를 보장하기 위한 강력한 매커니즘, 원칙 미준수로 인해 피해 입은 개인에 대한 해결책, 원칙 미준수 시 조직에 대한 영향 등이 포함되어야 함 - 이러한 매커니즘에는 다음이 포함되어야 함 i. 각 개인의 불만 사항과 분쟁을 조사하고 원칙을 참조하여 개인에게 무료로 신속하게 해결할 수 있는 쉽게 이용할 수 있는 독립적 해결 매커니즘과 해당 법률 또는 민간 부문 대책에서 제공하는 경우 부여되는 손해배상 ii. 조직이 개인 정보 보호 관행에 대해 하는 증명 및 주장이 사실인지, 개인 정보 보호 관행이 제시된 대로 이행되었는지, 특히 미준수 사례와 관련하여 확인을 위한 후속 절차 iii. 원칙 준수를 선언한 조직이 원칙을 준수하지 않아 발생하는 문제를 해결해야 할 의무 및 그러한 조직에 대한 제재 조치(제재는 조직이 규정을 준수할 수 있도록

	충분히 엄격해야 함)
b	- 조직 및 조직이 선정한 독립적인 해결 매커니즘은 EU-U.S. DPF와 관련된 정보에 대한 부처의 문의 및 요청에 신속하게 응답해야 함 - 모든 조직은 부처를 통해 EU 회원국 당국이 언급한 원칙 준수와 관련된 불만 사항에 신속하게 응답해야 함 - 인적 자원 데이터를 처리하는 조직을 포함하여 DPA와 협력하기로 선택한 조직은 불만 사항의 조사 및 해결과 관련하여 해당 당국에 직접 응답해야 함
c	- 개인이 해당 조직에 통지를 전달하고 부속서 1에 명시된 절차 및 조건에 따라 구속력 있는 중재를 요청하는 경우, 조직은 중재하고 부속서 1에 규정된 조건을 따라야 할 의무가 있음
d	- 제3자 이전의 맥락에서, 참여 조직은 EU-U.S. DPF에 따라 수령한 개인 정보 처리에 대해 책임을 지며, 이후 그 조직을 대신하여 대리인 역할을 하는 제3자에게 이전하는 것에 대해 책임을 짐 - 참여 조직은 대리인이 그러한 개인 정보를 원칙에 부합하지 않는 방식으로 처리할 경우, 해당 조직이 피해를 초래한 사건에 책임이 없음을 입증하지 않는 한, 원칙에 따라 책임을 짐
e	- 조직이 규정 미준수에 근거한 법원 명령, 미준수에 근거하여 원칙 또는 원칙의 향후 부속서에 등재될 법적 조직(예: FTC 또는 DOT)의 명령 대상이 되는 경우, 조직은 기밀성 요건에 부합하는 범위 내에서 법원 또는 미국 법정 기관에 제출한 규정 준수 또는 평가 보고서 관련 EU-U.S. DPF 관련 섹션을 공개해야 함 - 부처는 참여 조직의 준수 문제에 대해 DPA를 위한 전담 연락 창구를 구축하며, FTC 및 DOT는 부처 및 EU 회원국 당국이 보낸 원칙 미준수 건에 대한 의뢰를 우선적으로 고려하며, 기존 기밀성 제한에 따라 적시에 의뢰한 회원국 당국과 회부와 관련된 정보를 교환함

3 관련 법령 및 표준

□ 참조

○ Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance)

- 개인 데이터 처리 및 그러한 데이터의 자유로운 이동과 관련한 자연인 보호 및 지침 95/46/EC(일반 데이터 보호 규정) 폐지에 관한 2016년 4월 27일 유럽의회 및 유럽이사회 규정 (EU) 2016/679

○ Commission Implementing Decision (EU) 2016/1250 of 12 July 2016 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the EU-U.S. Privacy Shield (notified under document C(2016) 4176) (Text with EEA relevance)

- EU-U.S. 프라이버시 실드가 제공하는 보호의 적절성에 관한 유럽의회 및 이사회의 지침 95/46/EC에 따른 2016년 7월 12일의 위원회 이행 결정(EU) 2016/1250(문서 C(2016) 4176에 따라 통지)

붙임 **규제원문**

□ 부속서 1. 미국 상무부가 발표한 EU-U.S. 데이터 프라이버시 프레임워크 원칙

I. 개요

1. 미국과 유럽연합("EU")은 개인 정보 보호, 법치주의 및 각 시민, 경제 및 사회에 대한 범대서양 데이터 이동의 중요성에 대한 인식을 강화하기 위한 노력을 공유하지만, 미국은 개인 정보 보호에 대해 EU와는 다른 접근 방식을 취한다. 미국은 법률, 규정 및 자율 규제가 혼합된 부문별 접근 방식을 사용한다. 미국 상무부("부처")는 국제 상거래를 육성, 촉진 및 개발하기 위한 법적 권한에 따라 보충 원칙(집합적으로 "원칙") 및 원칙의 부록 I("부속서 I")를 포함한 EU-U.S. 데이터 프라이버시 프레임워크 원칙을 발행했다(15 U.S.C. § 1512). 이 원칙은 미국과 EU 간의 무역 및 상업을 촉진하기 위해 유럽 위원회(이하 "위원회"), 산업계 및 기타 이해 관계자와 협의하여 개발되었다. EU-U.S. 데이터 프라이버시 프레임워크("EU-U.S. DPF")의 핵심 구성 요소인 이 원칙은 EU에서 미국으로 개인 데이터 이전을 위한 신뢰할 수 있는 메커니즘을 미국 내 조직에 제공하는 동시에 EU 데이터 주체가 자신들의 개인 데이터가 비-EU 국가로 이전되었을 때 개인 데이터 처리와 관련하여 유럽 법률에서 요구하는 효과적인 안전장치 및 보호 혜택을 계속 받을 수 있도록 보장한다. 이 원칙은 "EU-U.S. DPF" 자격을 얻기 위한 목적으로 EU로부터 개인 데이터를 제공받고 따라서 위원회의 적정성 결정으로 이익을 얻는 미국의 적격 조직만이 사용하기 위한 것이다.[1] 이 원칙은 EU 회원국의 개인 데이터 처리에 적용되는 규정(EU) 2016/679("일반 데이터 보호 규정" 또는 "GDPR")[2]의 적용에 영향을 미치지 않는다. 해당 원칙은 미국법에 따라 적용되는 개인정보 보호 의무를 제한하지 않는다.

2. EU-U.S. DPF에 의존하여 EU로부터의 개인 데이터 이전을 효과적으로 수행하려면 조직은 부처(또는 부처의 지정자)에게 해당 원칙 준수를 자체-인증해야 한다. 따라서 "EU-U.S. DPF"에 가입하려는 조직의 결정은 전적으로 자발적이지만 실질적인 준수는 필수이다. 부처에 대해 자체-인증하고 원칙을 준수하겠다는 약속을 공개적으로 선언하는 조직은 원칙을 완전하게 준수해야 한다. "EU-U.S. DPF"에 가입하기 위해서는, (a) 연방통상위원회("FTC"), 미국 교통부("DOT") 또는 원칙 준수를 실질적으로 보장할 다른 법정 기관의 조사 및 집행 권한의 대상이 되어야 한다(*EU가 공인하는 기타 미국 법정 기관이 향후 부속서로 포함될 수 있다*), (b) 원칙 준수에 대한 약속을 공개적으로 선언한다, (c) 본 원칙에 따른 프라이버시(개인정보 보호) 방침을 공개한다. (d) 이를 완전하게 이행한다[3]. 조직의 원칙 미준수는 상업에서 불공정하거나 기만적인 행위 또는 상업에 영향을 미치는 불공정하거나 기만적인 행위를 금지하는 연방거래위원회(FTC)법 제5조에 따라 FTC에 의해 (15 U.S.C. § 45), 49 U.S.C. § 41712에 의거하여 항공운송인 또는 항공권 대리점이 항공운송 또는 항공운송의 판매에서 불공정하거나 기만적인 행위를 하는 것을 금지하는 DOT에 의해, 또는 그러한 행위를 금지하는 다른

---

[1] EU-U.S. DPF가 제공하는 보호의 적정성에 관한 위원회 결정이 아이슬란드, 리히텐슈타인 및 노르웨이에 적용되는 경우, EU-U.S. DPF는 이들 3개국뿐만 아니라 EU 모두를 포함할 것이다. 결과적으로 EU 및 EU 회원국에 대한 언급은 아이슬란드, 리히텐슈타인 및 노르웨이를 포함하는 것으로 해석된다.

[2] 지침 95/46/EC(일반 데이터 보호 규정)을 폐지하며, 개인 데이터 처리와 관련된 자연인 보호 및 해당 데이터의 자유로운 이동에 관한 2016년 4월 27일자 유럽의회 및 이사회 규정 (EU) 2016/679.

3 EU-U.S. 프라이버시 기본 원칙(EU-U.S. Privacy Shield Framework Principles)은 "EU-U.S. 데이터 프라이버시 기본 원칙(EU-U.S. Data Privacy Framework Principles)"으로 개정되었다(자체-인증에 관한 보충 원칙 *참조*).

법률 또는 규정에 의거하여 처벌가능하다. 조직의 원칙 미준수는 상업에서 불공정하거나 기만적인 행위 또는 상업에 영향을 미치는 불공정하거나 기만적인 행위를 금지하는 연방거래위원회(FTC)법 제5조에 따라 FTC에 의해 (15 U.S.C. § 45), 49 U.S.C. § 41712에 의거하여 항공운송인 또는 항공권 대리점이 항공운송 또는 항공운송의 판매에서 불공정하거나 기만적인 행위를 하는 것을 금지하는 DOT에 의해, 또는 그러한 행위를 금지하는 다른 법률 또는 규정에 의거하여 처벌가능하다.

3. 부처는 부서에 자체-인증을 하고 원칙("데이터 프라이버시 프레임워크 목록")을 준수하겠다는 약속을 선언한 미국 조직에 대한 신뢰할 수 있는 목록을 유지하고 대중에게 이를 제공한다. EU-U.S. DPF 혜택은 부처가 해당 조직을 데이터 프라이버시 프레임워크 목록에 올린 날로부터 보장된다. 부처는 EU-U.S. DPF에서 자발적으로 탈퇴하거나 부처에 연례 재-인증을 완료하지 못한 조직을 데이터 프라이버시 프레임워크 목록에서 삭제한다. 이러한 조직은 EU-U.S. DPF에 따라 받은 개인 정보에 대해 해당 원칙을 반드시 계속 적용해야 하고 연간 기준으로 부처에 그러한 약속을 확인해야 하며(즉, 해당 정보를 보유하는 한), 다른 공인된 수단(예: 위원회가 채택한 관련 표준 계약 조항의 요건을 완전히 반영하는 계약을 사용)을 통해 정보에 대해 "적절한" 보호를 제공하거나 정보를 반환 또는 삭제해야 한다. 부처는 또한 원칙을 지속적으로 준수하지 못한 조직을 데이터 프라이버시 프레임워크 목록에서 삭제할 것이다. 이러한 조직은 EU-U.S. DPF에 따라 받은 개인 정보를 반환하거나 삭제해야 한다. 조직이 데이터 프라이버시 프레임워크 목록에서 제거되면 더 이상 EU로부터 개인 정보를 받기 위한 위원회의 적정성 결정으로 혜택을 받을 자격이 없다.

4. 또한 부처는 이전에 부서에 대해 자체-인증을 받았으나 데이터 프라이버시 프레임워크 목록에서 제거된 미국 조직에 대한 권위 있는 기록을 유지하고 대중에게 제공할 것이다. 부처는 이러한 조직이 EU-U.S. DPF의 참가자가 아니며, 데이터 프라이버시 프레임워크 목록에서 제거된다는 것은 이러한 조직이 EU-U.S. DPF를 준수한다고 주장할 수 없으며, EU-U.S. DPF에 참여한다는 것을 암시하는 어떠한 진술이나 오해의 소지가 있는 관행도 피해야 한다는 것을 의미하며, 이러한 조직은 더 이상 EU로부터 개인 정보를 받기 위한 위원회의 적절성 결정으로 이익을 얻을 자격이 없다는 것을 의미하는 명확한 경고를 제공할 것이다. 데이터 프라이버시 프레임워크 목록에서 제거된 후 EU-U.S. DPF 참여를 계속 주장하거나 다른 EU-U.S. DPF 관련 잘못된 표현을 한 조직은 FTC, DOT 또는 기타 집행 당국의 집행 조치를 받을 수 있다.

5. 이러한 원칙의 준수는 (a) 법령 또는 정부의 규정이 상충되는 의무를 발생시키는 경우를 포함하여, 법원 명령을 준수하거나 공익, 법 집행 또는 국가 안보 요건을 충족하는 데 필요한 범위로 제한될 수 있다. (b) 법령, 법원의 명령, 또는 명백한 권한부여를 생성하는 정부 규정에 의해 제한될 수 있다. 단, 이러한 권한을 행사할 때 임의의 조직은 해당 원칙에 대한 비준수가 이러한 권한에 의해 진행되는 최우선적인 정당한 이익을 충족하는 데 필요한 범위 내에서 제한될 수 있다는 것을 입증할 수 있는 경우에 한한다. 또는 (c) GDPR에 명시된 조건 하에서 GDPR의 효력이 예외 또는 적용특례를 허용하는 경우 제한될 수 있다. 단, 그러한 예외 또는 적용특례는 비교 가능한 맥락에서 적용된다. 이러한 맥락에서, 개인정보와 시민의 자유를 보호하기 위한 미국법률의 안전조치에는 행정명령 제14086[4]호에 명시된 조건에 따라 해당 행정명령이 요구하는 것이 포함된다. 사생활 보호 강화라는 목표에 부합하여, 조직은 이러한 원칙을 완전하고 투명하게 구현하기 위해 노력해야 하며, 여기에는 위 (b)에 의해 허용된 원칙에 대한 예외가 적용되는 조직의 개인정보 보호정책에 표시하도록 노력해야

[4] 2022년 10월 7일자 행정 명령 "미국 신호 정보 활동에 대한 보호 강화"

한다. 같은 이유로, 원칙 및/또는 미국법에 따라 선택권(옵션)이 허용되는 경우, 조직은 가능한 한 더 높은 차원의 보호를 선택할 것으로 예상된다.

6. 조직은 EU-U.S. DPF에 가입한 후에는 EU-U.S. DPF에 의존하여 이전된 모든 개인 데이터에 원칙을 적용해야 한다. EU-U.S. DPF 혜택을 고용 관계의 맥락에서 사용하기 위해 EU에서 이전된 인사 개인정보로 확장하기로 선택한 조직은 부처에 대한 자체-인증 시 이를 표시해야 하며, 자체-인증에 관한 보충 원칙에 명시된 요건을 따라야 한다.

7. EU-U.S. DPF에 참여하는 조직이 원칙 및 관련 개인정보 보호정책을 해석하고 준수하는 문제에 대해서는 해당 조직이 EU 데이터 보호 당국("DPA")과 협력하기로 약속한 경우를 제외하고 미국 법이 적용된다. 달리 명시되지 않는 한, 원칙의 모든 조항은 관련이 있는 경우에 적용된다.

8. 정의:

a. "개인 데이터" 및 "개인 정보"는 GDPR 범위 내에 있는 식별되거나 식별 가능한 개인에 대한 데이터로, 미국의 조직이 EU로부터 수신하여 임의의 형태로 기록된 데이터이다.

b. 개인 데이터의 "처리"는 수집, 기록, 구성, 저장, 조정 또는 변경, 검색, 상담, 사용, 공개 또는 보급 또는 삭제 또는 폐기와 같이 자동화된 수단에 의한 것인지에 관계없이 개인 데이터에 대해 수행되는 모든 작업 또는 일련의 작업을 의미한다.

c. "컨트롤러"는 단독으로 또는 다른 이와 공동으로 개인 데이터 처리의 목적과 수단을 결정하는 개인 또는 조직을 의미한다.

9. 원칙 및 원칙의 부속서 I의 발효일은 유럽 위원회의 적정성 결정이 발효되는 날짜이다.

II. 원칙

1. 통지

a. 조직은 개인에게 다음 사항을 알려야 한다:

i. EU-U.S. DPF 참여 및 데이터 프라이버시 프레임워크 목록에 대한 링크 또는 웹 주소 제공,

ii. 수집된 개인 데이터의 유형 및 해당되는 경우 원칙을 준수하는 조직의 미국 법인 또는 미국 자회사,

iii. EU-U.S. DPF에 의존하여 EU로부터 받은 모든 개인 데이터에 대해 원칙에 따르겠다는 약속,

iv. 개인들에 대한 개인 정보를 수집하고 사용하는 목적

v. 문의 또는 불만 사항에 대응할 수 있는 EU 내 관련 사업장을 포함하여 문의 또는 불만 사항에 대해 조직에 연락하는 방법,

vi. 제3자에게 개인정보를 공개할 경우 제3자의 유형이나 신원, 및 공개의 목적,

vii. 자신의 개인 데이터를 열람할 수 있는 개인의 권리,

viii. 조직이 개인 데이터의 사용과 공개를 제한하기 위해 개인에게 제공하는 선택과 수단,

ix. 불만을 해결하고 개인에게 적절한 지원을 무료로 제공하기 위해 지정된 독립 분쟁 해결 기관 및 해당 기관에 대한 다음 여부 사항: (1) DPA에 의해 설립된 패널, (2) EU에 기반을 둔

대안적 분쟁 해결 제공자, (3) 미국에 기반을 둔 대안적 분쟁 해결 제공자,

x. FTC, DOT 또는 기타 미국의 권한이 있는 법적 기구의 조사 및 집행 권한의 대상이 됨,

xi. 특정 조건 하에서 개인이 구속력 있는 중재를 개시할 가능성,[5]

xii. 국가 안보 또는 법 집행 요건을 충족하는 것을 포함하여 당국의 합법적인 요청에 따라 개인 정보를 공개해야 하는 요건

xiii. 제3자에게 이전하는 경우의 책임.

b. 이 통지는 개인이 처음으로 조직에 개인 정보를 제공하도록 요청 받았을 때 또는 그 후 실행 가능한 한 빨리 제공해야 한다. 단 어떤 경우에도 그러나 조직이 정보를 이전하는 조직이 원래 수집 또는 처리한 목적 이외의 목적으로 해당 정보를 사용하거나 처음으로 제3자에게 공개하기 전에 제공해야 한다.

2. 선택

a. 조직은 개인에게 그들의 개인 정보가 (i) 제3자에게 공개될 것인지 (ii) 개인이 최초로 수집된 목적 또는 그 후에 승인한 목적과 실질적으로 다른 목적으로 사용될 것인지를 선택(즉, 옵트아웃)할 기회를 제공해야 한다. 개인은 선택권을 행사하기 위해 명확하고, 눈에 띄며, 쉽게 이용할 수 있는 메커니즘을 제공받아야 한다.

b. 전항에 대한 적용특례를 통해, 조직을 대신하여 또는 조직의 지시에 따라 업무를 수행하는 대리인 역할을 하는 제3자에게 정보를 공개할 경우, 선택권을 제공할 필요는 없다. 그러나, 조직은 항상 해당 대리인과 계약을 체결해야 한다.

c. 민감한 정보(즉, 의료 또는 건강 상태, 인종 또는 민족적 기원, 정치적 의견, 종교 또는 철학적 신념, 노동조합 가입을 명시하는 정보 또는 개인의 성생활을 명시하는 개인 정보)의 경우, 조직은 해당 정보를 제3자에게 공개하거나 (ii) 원래 수집 목적 또는 옵트인 선택권을 행사하여 이후에 개인이 승인한 목적 이외의 목적으로 사용할 경우 개인으로부터 승락에 대한 명시적 동의(즉, 옵트-인)를 얻어야 한다. 또한, 조직은 제3자가 식별하고 민감한 정보로 취급한 개인 정보를 전달받을 경우 이를 민감한 정보로 취급해야 한다.

3. 3자 이전에 대한 책임

a. 컨트롤러 역할을 하는 제3자에게 개인 정보를 이전하기 위해, 조직은 통지 및 선택 원칙(Notice and Choice Principles)을 준수해야 한다. 조직은 또한 개인이 제공한 동의에 부합하는 제한되고 특정된 목적을 위해서만 그러한 데이터를 처리할 수 있으며 수신자가 원칙과 동일한 수준의 보호를 제공할 것이며 더 이상 이러한 의무를 충족할 수 없다고 결정을 내릴 경우 조직에 통지할 것이라는 제3자 컨트롤러와 계약을 체결해야 한다. 해당 계약은 그러한 결정이 내려질 경우, 제3자 컨트롤러는 처리를 중단하거나 다른 합리적이고 적절한 조치를 취하여 시정할 것을 규정해야 한다.

b. 대리인 역할을 하는 제3자에게 개인 정보를 이전하기 위해, 조직은 (i) 제한되고 특정된 목적으로만 해당 데이터를 이전하고 (ii) 대리인이 원칙에 따라 요구되는 것과 최소한 동일한

[5] *예를 들어*, 청구, 집행 및 책임 원칙의 섹션 (c). 참조

수준의 개인 정보 보호를 제공할 의무가 있음을 확인하고, (iii) 대리인이 원칙에 따른 조직의 의무에 부합하는 방식으로 이전된 개인 정보를 효과적으로 처리할 수 있도록 합리적이고 적절한 조치를 취하고 (iv) 대리인이 더 이상 원칙에 따라 요구되는 수준의 보호를 제공할 의무를 충족할 수 없다고 결정하는 경우, 조직에 통보하고 (v) 통지 시 (iv)를 포함하여 승인되지 않은 처리를 중단하고 시정하기 위한 합리적이고 적절한 조치를 취하고 (vi) 요청 시 해당 대리인과 체결한 계약의 관련 개인 정보 보호 조항의 요약 또는 대표 사본을 부처에 제공해야 한다.

4. 보안

a. 개인정보를 생성, 유지, 사용 또는 배포하는 조직은 개인정보의 처리에 관련된 위험과 개인정보의 특성을 적절히 고려하여 개인정보의 손실, 오용 및 무단 접근, 공개, 변경 및 파기를 방지하기 위한 합리적이고 적절한 조치를 취해야 한다.

5. 데이터 무결성 및 목적 제한

a. 원칙에 따라, 개인 정보는 처리 목적과 관련된 정보로 제한되어야 한다.[6] 조직은 수집의 목적 또는 그 후에 개인이 승인한 목적과 양립할 수 없는 방법으로 개인 정보를 처리할 수 없다. 이러한 목적에 필요한 범위 내에서 조직은 개인 데이터가 의도된 용도에 대해 신뢰할 수 있고 정확하며 완전하고 최신 상태임을 보장하기 위해 합리적인 조치를 취해야 한다.

b. 정보는 5(a)의 의미 내에서 처리 목적에 부합하는 한 개인을 식별하거나 식별할 수 있도록 하는 형태[7]로만 보관될 수 있다. 이러한 의무는 조직이 공익 차원의 보관, 저널리즘, 문학 및 예술, 과학적 또는 역사적 연구 및 통계 분석 목적에 합당하게 부합하는 범위 내에서 개인 정보를 더 오랜 기간 동안 처리하는 것을 방해하지 않는다. 이러한 경우, 이러한 처리는 EU-U.S. DPF의 다른 원칙 및 조항의 적용을 받아야 한다. 조직은 이 조항을 준수하는 데 있어 합리적이고 적절한 조치를 취해야 한다.

6. 열람

a. 개인은 조직이 보유하고 있는 개인 정보를 열람할 수 있어야 하며, 해당 정보가 부정확하거나 원칙을 위반하여 처리된 경우에는 해당 정보를 수정, 개정 또는 삭제할 수 있어야 한다. 단, 열람 제공에 따른 부담 또는 비용이 해당 경우에 개인의 사생활에 대한 위험과 비례하지 않거나 해당 개인 이외의 다른 사람의 권리가 침해될 수 있는 경우는 제외한다.

7. 청구, 집행 및 책임

a. 효과적인 개인 정보 보호에는 원칙 준수를 보장하는 강력한 메커니즘, 원칙 비준수로 인해 영향을 받는 개인에 대한 청구권, 원칙을 따르지 않을 때 조직에 대한 결과가 포함되어야 한다. 최소한 그러한 메커니즘에는 다음이 포함되어야 한다:

---

[6] 상황에 따라, 적합한 처리 목적의 예로는 고객 관계, 규정 준수 및 법적 고려 사항, 감사, 보안 및 사기 방지, 조직의 법적 권리 보존 또는 방어 또는 정보 수집의 맥락을 고려하여 합리적인 기대에 부합하는 기타 목적을 포함할 수 있다.

[7] 이러한 맥락에서, 사용될 가능성이 상당히 높은 식별 수단(무엇보다도 식별에 필요한 비용과 시간, 처리 당시의 이용 가능한 기술을 고려할 때)과 데이터가 보관되는 형태를 고려할 때, 개인은 조직에 의해 합리적으로 식별될 수 있거나, 데이터를 열람할 수 있는 제3자가 있다면, 개인은 제3자에 의해 "식별 가능"하다.

i. 각 개인의 불만 및 분쟁을 조사하고 개인에게 비용을 들이지 않고 원칙을 참조하여 신속하게 해결하는 즉시 사용할 수 있는 독립적인 수단(청구) 메커니즘 및 해당 법률 또는 민간 부문 이니셔티브가 제공하는 경우 부여되는 손해 배상

ii. 조직이 개인정보 보호 관행에 대해 하는 증명 및 주장이 사실인지, 그리고 특히 미준수 사례와 관련하여 개인정보 보호 관행이 제시된 대로 이행되었는지 검증하기 위한 후속 절차

iii. 원칙 준수를 선언한 조직이 원칙을 준수하지 않아 발생하는 문제를 해결해야 할 의무 및 그러한 조직에 대한 제재 조치. 제재는 조직이 규정을 준수할 수 있도록 충분히 엄격해야 한다.

b. 조직 및 조직이 선정한 독립적인 수단(청구) 메커니즘은 EU-U.S. DPF와 관련된 정보에 대한 부처의 문의 및 요청에 신속하게 응답한다. 모든 기관은 부처를 통해 EU 회원국 당국이 언급한 원칙 준수와 관련된 불만 사항에 신속하게 응답해야 한다. 인적 자원 데이터를 처리하는 조직을 포함하여, DPA와 협력하기로 선택한 조직은 불만 사항의 조사 및 해결과 관련하여 해당 기관에 직접 응답해야 한다.

c. 개인이 문제가 된 조직에 통지를 전달하고 부속서 I에 규정된 절차와 조건에 따라 구속력 있는 중재를 요청할 경우, 조직은 청구를 중재하고 부속서 I에 규정된 조건에 따라야 할 의무가 있다.

d. 3자 이전(역외 이전)의 맥락에서, 참여 조직은 EU-U.S. DPF에 따라 수령한 개인 정보 처리에 대해 책임을 지며, 이후에 그 기관을 대신하여 대리인 역할을 하는 제3자에게 이전하는 것에 대해 책임을 진다. 참여 기관은 대리인이 그러한 개인 정보를 원칙에 부합하지 않는 방식으로 처리할 경우, 해당 기관이 피해를 초래한 사건에 책임이 없음을 입증하지 않는 한, 원칙에 따라 책임을 진다.

e. 조직이 비준수에 근거한 법원명령 또는 비준수에 근거하여 원칙 또는 원칙의 향후 부속서에 등재될 법적 기관(예: FTC 또는 DOT)의 명령의 대상이 되는 경우, 조직은 기밀성 요건에 부합하는 범위 내에서 법원 또는 미국의 법적 기관에 제출된 준수 또는 평가 보고서의 관련 EU-U.S. DPF 관련 섹션을 공개해야 한다. 부처는 참여 조직의 준수 문제에 대해 DPA를 위한 전용 연락 창구를 구축했다. FTC 및 DOT는 부처 및 EU 회원국 당국이 보낸 원칙 미준수 회부를 우선 심리하며, 기존 기밀성 제한에 따라 적시에 회부한 회원국 당국과 회부와 관련된 정보를 교환한다.

III. 보충 원칙

1. 민감한 데이터

a. 조직은 처리가 다음과 같은 경우 민감한 데이터와 관련하여 확실하고 명시적인 동의(즉, 옵트인)를 얻을 필요가 없다:

i. 데이터 주체 또는 타인의 중대한 이익에 부합하는 경우

ii. 법적 청구 또는 변호를 위해 필요한 경우

iii. 의료 서비스 또는 진단을 제공하기 위해 필요한 경우

iv. 정치적, 철학적, 종교적 또는 노동 조합 목적을 가진 재단, 협회 또는 기타 비영리 조직에 의해 정당한 활동 과정에서 수행되거나 처리가 전적으로 해당 조직의 구성원 또는 그 목적과 관련하여 조직과 정기적으로 연락하고 정보 주체의 동의 없이 데이터를 제3자에게 공개하지 않는 조건에서 수행되는 경우

v. 고용법률 분야에서 조직의 의무를 수행하는 데 필요한 경우

vi. 개인이 명시적으로 공개한 데이터와 관련된 경우.

2. 저널리즘 예외

a. 미국 수정 헌법 제1조에 구체화된 자유 언론의 권리가 사생활 보호 이익과 교차하는 언론 자유에 대한 미국 헌법의 보호를 고려할 때 수정 헌법 제1조는 미국 개인 또는 조직의 활동과 관련하여 이러한 이익의 균형을 규율해야 한다.

b. 사용 여부와 상관없이 언론 자료의 출판, 방송 또는 기타 형태의 대중 커뮤니케이션을 위해 수집된 개인 정보와 미디어 아카이브에서 유포된 이전에 출판된 자료에서 발견된 정보는 해당 원칙의 요건이 적용되지 않는다.

3. 2차적 책임

a. 인터넷 서비스 제공자("ISP"), 통신 사업자 및 기타 조직은 다른 조직을 대신하여 정보를 단지 이전, 라우팅, 전환 또는 캐시(단순 저장)할 경우 해당 원칙에 따른 책임을 지지 않는다. EU-U.S. DPF는 2차 책임을 생성하지 않는다. 조직이 제3자에 의해 이전되는 데이터의 통로 역할을 하고 있고 해당 개인 데이터를 처리하는 목적과 수단을 결정하지 않는 범위 내에서 책임을 지지 않는다.

4. 실사 수행 및 감사 수행

a. 감사인 및 투자 은행가의 활동에는 개인의 동의 또는 인지 없이 개인 데이터를 처리하는 것이 포함될 수 있다. 이는 아래에 설명된 상황에서 통지, 선택 및 열람 원칙에 따라 허용된다.

b. 참여 조직을 포함하여, 공개 주식회사 및 비공개 회사는 정기적으로 감사를 받는다. 특히 잠재적인 불법 행위를 조사하는 감사는 조기에 공개될 경우 위험에 처할 수 있다. 마찬가지로 잠재적인 합병 또는 인수에 참여하는 조직은 "실사" 검토를 수행하거나 대상이 되어야 한다. 이는 종종 고위 임원 및 기타 주요 인사에 대한 정보와 같은 개인 데이터의 수집 및 처리를 수반한다. 조기 공개는 거래를 방해하거나 해당 증권 규정을 위반할 수도 있다. 실사에 종사하는 투자 은행가 및 변호사 또는 감사를 수행하는 감사인은 법적 또는 공익 요건을 충족하는 데 필요한 범위와 기간 동안 그리고 이 원칙의 적용이 조직의 정당한 이익을 해칠 수 있는 기타 상황에서만 개인에게 알리지 않고 정보를 처리할 수 있다. 이러한 정당한 이익에는 조직의 법적 의무 준수 및 합법적인 회계 활동 모니터링, 가능한 인수, 합병, 합작 투자 또는 투자 은행가 또는 감사인이 수행하는 기타 유사한 거래와 관련된 기밀 유지의 필요성이 포함된다.

5. 데이터 보호 당국의 역할

a. 조직은 아래에 설명된 대로 DPA와 협력하겠다는 약속을 이행한다. EU-U.S. DPF 하에서, EU로부터 개인 데이터를 받는 미국의 조직은 원칙 준수를 보장하기 위한 효과적인

메커니즘을 사용하기 위해 노력해야 한다. 보다 구체적으로 청구, 집행 및 책임 원칙에 명시된 대로 참여 조직은 다음을 제공해야 한다: (a)(i) 데이터와 관련된 개인에 대한 청구 (a)(ii) 개인정보 보호 관행에 대한 조직의 증명 및 주장이 사실인지 확인하기 위한 후속 절차 (a)(iii) 원칙을 준수하지 않아 발생하는 문제를 해결해야 할 의무 및 해당 조직에 대한 결과(대가). 조직은 DPA와 협력하기 위해 여기에 명시된 요건을 준수하는 경우 청구, 집행 및 책임 원칙의 (a)(i) 및 (a)(iii) 항을 충족할 수 있다.

b. 조직은 부처에 대한 EU-U.S. DPF 자체-인증 제출서에서 다음을 선언함으로써 DPA와 협력할 것을 약속한다(자체-인증에 관한 보충원칙 참조):

i. 조직이 청구, 집행 및 책임 원칙의 (a)(i)와 (a)(iii)의 요건을 충족할 것을 결정한다.

ii. 원칙에 따라 제기된 불만의 조사 및 해결에 DPA와 협력한다.

iii. 조직은 원칙을 준수하지 않음으로써 영향을 받는 개인의 이익을 위한 구제 또는 보상 조치를 포함하여 원칙을 준수하기 위해 조직은 특정 조치를 취해야 한다는 DPA의 조언을 준수하며 DPA에게 해당 조치가 취해졌다는 서면 확인서를 제공한다.

c. <u>DPA 패널의 작업</u>

i. DPA의 협력은 다음과 같은 방법으로 정보와 조언의 형태로 제공된다:

1. DPA의 조언은 EU 차원에서 설립된 DPA의 비공식 패널을 통해 전달될 것이며, 이는 특히 조화롭고 일관된 접근 방식을 보장하는 데 도움이 될 것이다.

2. 패널은 EU-U.S. DPF에 따라 EU로부터 이전된 개인 정보 처리에 대한 개인의 해결되지 않은 불만에 대해 관련된 미국 조직에 조언을 제공할 것이다. 이 조언은 원칙이 올바르게 적용되고 있는지 확인하기 위한 것이며 DPA가 적절하다고 간주하는 관련 개인에 대한 모든 구제조치가 포함할 것이다.

3. 패널은 관련 조직으로부터 회부 및/또는 EU-U.S. DPF목적으로 DPA와 협력하기로 약속한 조직에 대해 개인으로부터 직접 받은 불만에 대응하여 조언을 제공하고 이러한 개인이 1차적으로 해당 조직이 제공할 수 있는 자체 불만 처리 제도를 사용하도록 권장하고 필요한 경우 도움을 줄 것이다.

4. 조언은 분쟁의 양측이 의견을 제시하고 원하는 증거를 제공할 수 있는 합리적인 기회를 얻은 후에만 발표된다. 패널은 적절한 절차에 대한 이 요건이 허용하는 한 신속하게 조언을 전달하려고 할 것이다. 일반적으로 패널은 불만 또는 회부를 받은 후 60일 이내에 그리고 가능한 한 신속하게 조언을 제공하는 것을 목표로 한다.

5. 패널은 적합하다고 판단될 경우, 패널에 제출된 불만 사항에 대한 심리 결과를 공개한다.

6. 패널을 통한 조언 전달은 패널 또는 개별 DPA에 대해 그 어떤 책임도 발생시키지 않는다.

ii. 위에서 언급한 바와 같이, 분쟁 해결을 위해 이 옵션을 선택하는 기관은 DPA의 조언을 준수하기로 약속해야 한다. 만약 어떤 조직이 조언이 전달된 후 25일 이내에 이를 준수하지 않고 지연에 대해 만족스러운 설명을 제시하지 않은 경우, 패널은 FTC, DOT 또는 기만

또는 잘못된 표현의 경우에 집행 조치를 취할 수 있는 법적 권한을 가진 다른 미국 연방 또는 주 기관에 문제를 회부하거나 협력하기로 한 합의가 심각하게 위반되었으므로 무효로 간주되어야 한다는 결론을 내리는 의도를 통지할 것이다. 후자의 경우, 패널은 데이터 프라이버시 프레임워크 목록이 정당하게 수정될 수 있도록 부처에 통지할 것이다. 원칙 미준수뿐 만 아니라 DPA와 협력하기로 한 약속을 이행하지 않을 경우, FTC 법 제5조(15 U.S.C. § 45), 49 U.S.C. § 41712 또는 다른 유사한 법령에 따라 기만적인 관행을 이유로 조치가 취해질 수 있다.

d. 고용 관계의 맥락에서 EU로부터 이전된 인사 데이터를 포함하기 위해 EU-U.S. DPF 혜택을 원하는 기관은 해당 데이터와 관련하여 DPA와 협력할 것을 약속해야 한다(인사 데이터 보충 원칙 참조).

e. 이 옵션을 선택한 조직은 연간 수수료를 지불해야 하며, 이는 패널의 운영 비용을 충당하기 위한 것이다. 조직은 조직에 대한 회부 또는 불만사항에 대한 패널의 심리로 인해 발생하는 필요한 번역 비용을 충족하도록 추가로 요청 받을 수 있다. 수수료 금액은 위원회와의 협의를 거쳐 부처가 결정한다. 수수료 징수는 부처가 이 목적을 위해 징수된 자금의 보관자 역할로 선정한 제3자에 의해 수행될 수 있다. 부처는 수수료를 통해 징수된 자금의 분배를 위한 적절한 절차 및 패널의 기타 절차적 및 행정적 측면에 대해 위원회 및 DPA와 긴밀히 협력할 것이다. 부처와 위원회는 수수료 징수 빈도에 대한 변경을 합의할 수 있다.

6. 자체-인정

a. EU-U.S. DPF 혜택은 부처가 조직을 데이터 프라이버시 프레임워크 목록에 올린 날로부터 보장된다. 부처는 조직의 초기 자체-인증 제출이 완료되었다고 결정한 후에만 데이터 프라이버시 프레임워크 목록에 조직을 등록하고, 조직이 자발적으로 탈퇴하거나, 연간 재인증을 완료하지 못하거나, 지속적으로 원칙을 준수하지 못할 경우 해당 목록에서 해당 조직을 제거한다(분쟁 해결 및 집행에 관한 보충 원칙 참조)

b. EU-U.S. DPF에 대해 최초로 자체-인증 또는 이후 재-인증하기 위해, 조직은 원칙[8] 준수를 자체-인증 또는 재-인증하고 있는 조직을 대신하여 해당 기업의 임원은 부처에 최소한 다음과 같은 정보가 포함된 제출서를 제공해야 한다:

i. 자체-인증 또는 재-인증하는 미국 조직의 이름과 해당 조직이 다루고자 하는 원칙을 준수하는 조직의 미국 기업 또는 미국 자회사의 이름.

ii. EU-U.S. DPF에 따라 EU로부터 받을 개인 정보와 관련된 조직의 활동에 대한 설명.

iii. 다음을 포함하여 개인 정보에 대한 조직의 관련 개인 정보 보호 정책에 대한 설명:

1. 조직이 공개 웹사이트를 가지고 있는 경우, 개인정보 보호 정책이 제공되는 관련 웹 주소, 조직이 공개 웹사이트를 가지고 있지 않는 경우, 일반인이 볼 수 있도록 개인정보 보호 정책이 제공되는 장소.

2. 그 시행일

[8] 제출은 원칙 준수와 관련하여 조직 및 조직의 적용 대상 회사를 대표할 권한이 있는 조직 내 개인이 부처의 데이터 프라이버시 프레임워크 웹 사이트를 통해 이루어져야 한다.

iv. 다음을 포함하여 원칙 [9]에 따라 발생하는 불만, 열람 요청 및 기타 문제를 처리하기 위한 조직 내 연락 사무소:

1. 조직 내 관련 개인 또는 관련 연락 사무소의 이름, 직책(해당되는 경우), 이메일 주소 및 전화 번호

2. 조직의 관련 미국 우편 주소

v. 가능한 불공정하거나 기만적인 관행 및 사생활을 규율하는 법률 또는 규정의 위반과 관련하여 조직에 대한 청구를 심리할 관할권이 있는 특정 법정 기관(원칙 또는 향후 원칙 부속서에 등재된 기관)

vi. 조직이 회원인 개인 정보 보호 프로그램의 이름

vii. 검증 방법(즉, 자체 평가 또는 이러한 검토를 완료한 제3자를 포함한 외부 규정 준수 검토)[10]

viii. 해결되지 않은 원칙 관련 불만 사항을 조사할 수 있는 관련된 독립 청구 메커니즘.[11]

c. 조직이 고용 관계의 맥락에서 사용할 목적으로 EU-U.S. DPF 의 혜택에 EU로부터 이전된 인적 자원 정보가 포함되기를 희망하는 경우, 원칙 또는 원칙의 향후 부속서에 등재된 법정 기관이 인적 자원 정보 처리 과정에서 발생하는 조직에 대한 청구를 심리할 관할권이 있는 경우, 조직은 그렇게 할 수 있다. 또한, 조직은 최초 자체-인증 제출서 및 재-인증 제출서에 이를 표시해야 하며, 인적 자원 데이터에 관한 보충 원칙 및 데이터 보호 당국의 역할(해당하는 경우)에 따라 EU 당국 또는 관련 당국과 협력하겠다는 약속을 선언하고 해당 당국이 제공한 조언을 준수할 것임을 선언한다. 조직은 또한 영향을 받는 직원이 개인 정보 보호 정책을 볼 수 있는 곳에 대한 정보를 부처에 제공해야 한다.

d. 부처는 완료된 최초 자체-인증 제출서를 제출한 조직들의 데이터 프라이버시 프레임워크 목록을 유지 및 공개하며, 완료된 연간 재-인증 제출서 및 분쟁 해결 및 집행에 관한 보충 원칙에 따라 접수된 통지를 기준으로 목록을 업데이트한다. 이러한 재-인증 제출서는 적어도 매년 제공되어야 한다. 그렇지 않을 경우 조직은 데이터 프라이버시 프레임워크 목록에서 제거되고 EU-U.S. DPF 혜택이 더 이상 보장되지 않는다. 부처에 의해 데이터 프라이버시 프레임워크 목록에 등재된 모든 조직은 통지 원칙을 준수하는 관련 개인 정보 보호 정책을 보유해야 하며 이러한 개인 정보 보호 정책에 원칙을 준수한다고 명시해야 한다.[12] 온라인에서 제공되는 경우 조직의 개인 정보 보호 정책에는 부처의 데이터 프라이버시 프레임워크 웹 사이트에 대한 하이퍼링크와 해결되지 않은 원칙 관련 불만 사항을 개인에게 무료로 조사할 수 있는 독립된 청구 메커니즘의 웹 사이트 또는 불만 제출 양식에 대한 하이퍼링크가 포함되어야 한다.

---

[9] 기본 "조직 연락처" 또는 "조직 기업 담당자"는 조직 외부에 있을 수 없다(예: 외부 고문 또는 외부 컨설턴트).

[10] 검증에 관한 보충 원칙 *참조*.

[11] 분쟁 해결 및 집행에 관한 보충 원칙 *참조*.

[12] 처음으로 자체-인증하는 조직은 부처가 조직에 그렇게 하라고 통보할 때까지 조직의 최종 개인 정보 보호 정책에 EU-U.S. DPF의 참여를 주장할 수 없다. 조직은 최초 자체-인증을 제출할 때 원칙에 부합하는 개인 정보 보호 정책 초안을 부처에 제공해야 한다. 부처가 조직의 최초 자체-인증 제출이 완료되었다고 결정하면 부처는 해당 조직에게 EU-U.S. DPF에 일치 개인 정보 보호 정책을 확정(예: 해당되는 경우 게시)해야 한다고 통보한다. 조직은 관련 개인 정보 보호 정책이 확정되는 즉시 부처에 즉시 통지해야 하며, 이때 부처는 조직을 데이터 프라이버시 프레임워크 목록에 등재한다.

e. 원칙은 자체-인증 즉시 적용된다. 이전에 EU-U.S. 프라이버시 프레임워크 원칙에 대해 자체-인증한 참여 조직은 "EU-U.S. 데이터 프라이버시 프레임워크 원칙"을 참조하도록 개인정보 보호 정책을 업데이트해야 한다. 이러한 조직은 가능한 한 빨리, 그리고 EU-U.S. 데이터 프라이버시 프레임워크 원칙 시행일로부터 최소 3개월 이내에 이 참조를 포함해야 한다.

f. 조직은 EU-U.S. DPF에 따라 EU로부터 받은 모든 개인 데이터에 대해 원칙을 적용해야 한다. 원칙을 준수한다는 약속은 해당 조직이 EU-U.S. DPF의 혜택을 누리는 기간 동안 수령한 개인 데이터와 관련하여 시간에 제한을 두지 않는다. 즉 그 약속은 해당 조직이 이후 어떠한 이유로 EU-U.S. DPF를 떠나더라도 해당 데이터를 저장, 사용 또는 공개하는 한 해당 데이터에 원칙이 계속 적용된다는 것을 의미한다. EU-U.S. DPF에서 탈퇴하고자 하는 조직은 부처에 해당 사실에 대해 미리 통지해야 한다. 이 통지는 해당 조직이 EU-U.S. DPF에 의존하여 받은 개인 데이터에 대해 무엇을 할 것인지(즉, 해당 데이터를 보유, 반환 또는 삭제할 것인지, 만약 해당 데이터를 보유할 경우 해당 데이터에 대해 보호를 제공하는 허가된 수단)를 또한 표시해야 한다. EU-U.S. DPF에서 탈퇴하지만 해당 데이터를 유지하려는 조직은 원칙을 데이터에 계속 적용하겠다는 약속을 매년 부서에 확언하거나 다른 승인된 수단(예: , 위원회가 채택한 관련 표준 계약 조항의 요건을 완전히 반영하는 계약 사용)을 통해 데이터에 대한 "적절한" 보호를 제공해야 한다. 그렇지 않으면 해당 조직은 해당 정보를 반환하거나 삭제해야 한다.[13] EU-U.S. DPF에서 탈퇴하는 조직은 관련 개인 정보 보호 정책에서 해당 조직이 EU-U.S. DPF에 계속 참여하고 있으며 그 혜택을 받을 자격이 있음을 의미하는 모든 참조를 제거해야 한다.

g. 합병, 인수, 파산 또는 청산의 결과와 같은 법인 지위의 변경으로 인해 별도의 법인으로 존재하지 않게 될 조직은 사전에 이 사실을 부처에 통지해야 한다. 통지에는 법인 지위의 변경으로 인해 발생한 조직이 (i) 기존 자체-인증을 통해 EU-U.S. DPF에 계속 참여할 것인지, (ii) EU-U.S. DPF의 새로운 참여자로 자체-인증할 것인지(예: 신규 회사 또는 존속 회사가 EU-U.S. DPF에 참여할 수 있는 기존 자체-인증을 이미 가지고 있지 않은 경우) 또는 (iii) 해당 조직이 EU-U.S. DPF에 따라 받고 향후 유지될 모든 개인 데이터에 대한 원칙의 지속적인 적용을 보장하는 서면 동의와 같은 다른 보호 조치를 마련할 것인지 표시해야 한다. (i), (ii) 또는 (iii) 중 어느 것도 적용되지 않는 경우, EU-U.S. DPF에 따라 받은 모든 개인 데이터는 즉시 반환되거나 삭제되어야 한다.

h. 조직이 어떠한 이유로 EU-U.S. DPF를 탈퇴할 경우, 조직이 EU-U.S. DPF에 계속 참여하거나 EU-U.S. DPF의 혜택을 받을 권리가 있음을 암시하는 모든 문구를 제거해야 한다. EU-U.S. DPF 인증 마크가 사용되는 경우, 또한 제거되어야 한다. 조직의 원칙 준수와 관련하여 일반 대중에게 잘못된 표현을 하는 경우, FTC, DOT 또는 기타 관련 정부 기관에 의해 조치될 수 있다. 부처에 대한 잘못된 표현은 거짓 진술에 관한 법률(U.S.C. § 1001)에 따라 조치될 수 있다.

---

[13] 조직이 탈퇴 시점에 EU-U.S. DPF에 의존하여 받은 개인 데이터를 보유하기로 선택하고 매년 해당 데이터에 원칙을 계속 적용한다고 부처에 확언하는 경우, 조직은 탈퇴 이후 매년 한 번 부처에 대해 (즉, 조직이 다른 허가된 수단을 통해 해당 데이터에 대해 "적절한" 보호를 제공하거나 해당 데이터를 반환하거나 삭제하고 해당 조치를 부처에 통보하지 않는 한) 해당 개인 데이터에 대해 무엇을 했는지, 계속 보유하고 있는 개인 데이터를 가지고 무엇을 할 것인지, 원칙 관련 질문에 대한 지속적인 연락 창구 역할을 할 사람은 누구인지 확인해 주어야 한다.

7. 검증

a. 조직은 EU-U.S. DPF 개인 정보 보호 관행에 대해 제기하는 증명과 주장이 사실이며 그러한 개인 정보 보호 관행이 언급된 대로 그리고 원칙에 따라 이행되었는지 확인하기 위한 후속 절차를 제공해야 한다.

b. 청구, 집행 및 책임 원칙의 검증 요건을 충족하기 위해, 조직은 자체-평가 또는 외부 규정 준수 검토를 통해 이러한 증명 및 주장을 입증해야 한다.

c. 조직이 자체-평가를 선택한 경우, 그러한 검증은 EU로부터 받은 개인 정보에 관한 개인 정보 보호 정책이 정확하고, 포괄적이며, 쉽게 이용할 수 있으며, 원칙에 부합하며, 완전히 이행되고 있음(즉, 준수되고 있음)을 입증해야 한다. 또한 개인에게 불만 사항을 처리하기 위한 사내 제도와 불만 사항을 진행할 수 있는 독립적인 청구 메커니즘에 대한 정보가 제공되고, 직원을 교육하고, 이를 준수하지 않을 경우 징계하는 절차가 마련되어 있으며, 위의 준수 사항에 대한 객관적인 검토를 주기적으로 수행하기 위한 내부 절차가 마련되어 있음을 표시해야 한다. 자체-평가가 완료되었음을 입증하는 진술서는 기업 임원 또는 기타 허가된 조직의 대표자에 의해 연 1회 이상 서명되어야 하며, 개인의 요청이 있거나 조사 또는 비준수에 대한 불만제기의 맥락에서 제공되어야 한다.

d. 조직이 외부 규정 준수 검토를 선택한 경우, 그러한 검증은 EU로부터 받은 개인 정보에 관한 개인 정보 보호 정책이 정확하고 포괄적이며 즉시 사용 가능하고 원칙을 준수하며 완전히 이행(즉, 준수되고 있음)됨을 입증해야 한다. 또한 개인이 불만 사항을 처리할 수 있는 메커니즘에 대해 통보 받았다는 사실을 나타내야 한다. 검토 방법에는 감사, 무작위 검토, "미끼(decoy)" 사용 또는 적절한 기술 도구 사용이 포함될 수 있지만 이에 국한되지 않는다. 외부 규정 준수 검토가 성공적으로 완료되었음을 확인하는 진술서는 검토자나 회사 임원 또는 조직의 다른 권한 있는 대표자가 최소 1년에 한 번 서명해야 하며 개인의 요청 시 또는 조사 또는 규정 준수에 대한 불만제기 맥락에서 사용할 수 있어야 한다.

e. 조직은 EU-U.S. DPF 프라이버시 관행의 이행에 대한 기록을 유지해야 하며, 조사 또는 비-준수에 대한 불만제기의 맥락에서 요청이 있을 시, 불만 조사를 담당하는 독립 분쟁 해결 기관 또는 불공정 및 기만적인 관행에 대해 관할권을 가진 기관에 이를 사용할 수 있도록 해야 한다. 조직은 또한 조직의 원칙 준수와 관련하여 부처의 문의 및 기타 정보 요청에 즉시 응답해야 한다.

8. 열람

a. <u>실제 열람 원칙</u>

i. 원칙에 따르면 열람권은 사생활 보호의 기본이다. 특히 열람권을 통해 개인은 자신에 대해 보유한 정보의 정확성을 확인할 수 있다. 열람 원칙은 개인이 다음과 같은 권리를 갖는 것을 의미한다:

1. 조직이 그들과 관련된 개인 데이터를 처리하고 있는지에 대한 확인을 조직으로부터 받을 권리[14]

[14] 조직은 처리 목적, 관련 개인 데이터 범주, 개인 데이터가 공개되는 수신자 또는 수신자 범주에 관한 개인의 요청에 응답해야 한다.

2. 그 처리의 정확성과 합법성을 확인할 수 있도록 개인들이 그러한 데이터를 전달받을 권리.

3. 데이터가 정확하지 않거나 원칙을 위반하여 처리되는 경우 데이터를 수정, 개정 또는 삭제할 권리.

ii. 개인은 자신의 개인 데이터에 대한 열람 요청을 정당화할 필요가 없다. 개인의 열람 요청에 응답할 때 조직은 먼저 요청을 초래한 문제에 따라 안내를 받아야 한다. 예를 들어 열람 요청이 모호하거나 범위가 넓은 경우 조직은 요청 동기를 더 잘 이해하고 응답 정보를 찾기 위해 개인을 대화에 참여시킬 수 있다. 조직은 개인이 조직의 어떤 부분과 상호작용했는지 또는 열람 요청의 대상이 되는 정보의 특성 또는 사용에 대해 문의할 수 있다.

iii. 열람의 기본 특성에 따라 조직은 열람을 제공하기 위해 항상 선의의 노력을 기울여야 한다. 예를 들어 특정 정보를 보호해야 하고 열람 요청 대상인 다른 개인 정보와 쉽게 분리할 수 있는 경우 조직은 보호된 정보를 수정하고 다른 정보를 사용할 수 있도록 해야 한다. 조직이 특정 상황에서 열람을 제한해야 한다고 결정하는 경우 열람을 요청하는 개인에게 그러한 결정을 내린 이유에 대한 설명과 추가 문의를 위한 연락처를 제공해야 한다.

b. 열람 제공의 부담 또는 비용

i. 개인 데이터에 대한 열람 권한은 해당 개인 이외의 사람의 정당한 권리가 침해되거나 열람 제공의 부담이나 비용이 해당 사례에서 개인의 사생활에 대한 위험에 비례하지 않는 예외적인 상황에서 제한될 수 있다. 비용과 부담은 중요한 요소이며 고려되어야 하지만 열람 제공이 합리적인지를 결정하는 제어 요소는 아니다.

ii. 예를 들어, 개인 정보가 개인에게 중대한 영향을 미치는 결정(예: 보험, 모기지 또는 직업과 같은 중요한 혜택의 거부 또는 부여)에 사용되는 경우 이 보충 원칙의 다른 조항과 일관되게 조직은 제공하기가 상대적으로 어렵거나 비용이 많이 드는 경우에도 해당 정보를 공개해야 한다. 요청된 개인 정보가 민감하지 않거나 개인에게 중대한 영향을 미치는 결정에 사용되지는 않지만 쉽게 사용할 수 있고 저렴하게 제공할 수 있는 경우 조직은 해당 정보에 대한 열람을 제공해야 한다.

c. 기밀 상업 정보

i. 기밀 상업 정보는 공개가 시장에서 경쟁업체에게 도움이 될 수 있는 경우 조직이 공개로부터 보호하기 위한 조치를 취한 정보이다. 조직은 완전한 열람 권한을 부여할 경우 조직에서 생성한 마케팅 추론 또는 분류와 같은 자체 기밀 상업 정보 또는 계약상 기밀 유지 의무가 적용되는 타인의 기밀 상업 정보가 공개되는 범위에 대해 열람을 거부하거나 제한할 수 있다.

ii. 비밀 상업 정보가 열람 요청의 대상이 되는 다른 개인 정보와 쉽게 분리될 수 있는 경우, 조직은 비밀 상업 정보를 편집하여 비밀이 아닌 정보를 이용할 수 있도록 해야 한다.

d. 데이터베이스 구성

i. 열람은 조직이 개인에게 관련 개인 정보를 공개하는 형태로 제공할 수 있으며, 개인이

조직의 데이터베이스에 대한 열람을 필요로 하지 않는다.

ii. 열람은 조직이 개인정보를 저장하는 범위에서만 제공되어야 한다. 열람 원칙은 그 자체로 개인정보 파일을 존속, 유지, 재조직 또는 재구성할 의무를 발생시키지 않는다.

e. 열람이 제한될 수 있는 경우

i. 조직은 개인에게 자신들의 개인 데이터에 대한 열람을 제공하기 위해 항상 선의의 노력을 다해야 하기 때문에 조직이 이러한 열람을 제한할 수 있는 상황은 제한적이며, 열람을 제한하는 모든 이유는 구체적이어야 한다. GDPR에 따라 조직은 공개가 국가 안보, 국방 또는 공공 안보과 같은 중요한 상쇄되는 중요한 공익의 보호를 방해할 가능성이 있는 경우 정보에 대한 열람을 제한할 수 있다. 또한 개인 정보가 연구 또는 통계 목적으로만 처리되는 경우 열람이 거부될 수 있다. 열람을 거부하거나 제한하는 다른 이유는 다음과 같다:

1. 범죄의 예방, 조사 또는 적발 또는 공정한 재판을 받을 권리를 포함하여 법의 실행 또는 집행 또는 사적 소송 사유에 대한 방해
2. 타인의 정당한 권리나 중대한 이익을 침해할 우려가 있는 경우의 공개
3. 법적 또는 기타 직업상의 특권이나 의무를 위반하는 행위
4. 직원 보안 조사 또는 고충 처리 절차를 방해하거나 직원 승계 계획 및 기업 개편과 관련, 또는
5. 건전한 경영과 관련된 모니터링, 조사 또는 규제 기능 또는 조직과 관련된 향후 또는 진행 중인 협상에 필요한 기밀 유지를 침해하는 행위.

ii. 예외를 주장하는 조직은 그 필요성을 입증할 책임이 있으며, 열람을 제한하는 이유와 추가 문의를 위한 연락처를 개인에게 제공해야 한다.

f. 확인을 받을 권리 및 열람 제공 비용을 충당하기 위한 수수료 청구

i. 개인은 이 조직이 자신과 관련된 개인정보를 가지고 있는지에 대한 확인을 받을 권리가 있다. 개인은 또한 자신과 관련된 개인정보에 대해 연락 받을 권리가 있다. 조직은 과도하지 않은 수수료를 부과할 수 있다.

ii. 예를 들어, 특히 반복된 요청 등 열람 요청이 명백하게 과도한 경우 수수료를 부과하는 것은 정당화될 수 있다.

iii. 개인이 비용을 지불하겠다고 제안하는 경우 비용을 이유로 열람을 거부할 수 없다.

g. 반복적이거나 성가신(남용되는) 열람 요청

i. 조직은 주어진 기간 내에 특정 개인의 열람 요청이 충족되는 횟수에 대한 합리적인 제한을 설정할 수 있다. 이러한 제한을 설정할 때 조직은 정보 업데이트 빈도, 데이터 사용 목적 및 정보의 특성과 같은 요소를 고려해야 한다.

h. 사기성 열람 요청

i. 요청하는 사람의 신원을 확인할 수 있는 충분한 정보가 제공되지 않는 한 조직은 열람을

제공할 필요가 없다.

i. 응답 기간

i. 조직은 합리적인 시간 내에 합리적인 방식으로 개인이 쉽게 이해할 수 있는 형식으로 열람 요청에 응답해야 한다. 정기적으로 데이터 주체에게 정보를 제공하는 조직은 과도한 지연이 발생하지 않는 한 정기적인 공개로 개별 열람 요청을 충족시킬 수 있다.

9. 인적 자원(인사) 데이터

a. "EU-U.S. DPF"의 적용범위

i. EU에 있는 조직이 고용 관계의 맥락에서 수집된 직원(과거 또는 현재 직원)에 대한 개인 정보를 EU-U.S. DPF에 참여하는 미국의 부모, 계열사 또는 비계열 서비스 제공자에게 이전하는 경우, 이전은 EU-U.S. DPF의 혜택을 누린다. 이러한 경우, 이전 전 정보의 수집과 처리는 해당 정보가 수집된 EU 회원국의 국내법의 적용을 받게 되며, 해당 법률에 따른 이전 조건 또는 제한이 존중되어야 한다.

ii. 해당 원칙은 개별적으로 식별되거나 식별 가능한 기록이 이전되거나 열람되는 경우에만 관련이 있다. 집계된 고용 데이터에 의존하고 개인 데이터를 포함하지 않거나 익명화된 데이터를 사용하는 통계 보고는 개인정보보호 관련 문제를 제기하지 않는다.

b. 통지 및 선택 원칙의 적용

i. EU-U.S. DPF에 따라 EU로부터 고용원 정보를 받은 미국 조직은 통지 및 선택 원칙에 따라 제3자에게 공개하거나 다른 목적으로만 사용할 수 있다. 예를 들어, 조직이 고용 관계를 통해 수집한 개인 정보를 마케팅 커뮤니케이션과 같은 비고용 관련 목적으로 사용하고자 하는 경우, 미국 조직은 개인이 그러한 목적을 위한 정보의 사용을 미리 승인하지 않은 경우, 그러한 목적을 달성하기 전에 해당 개인에게 필요한 선택권을 제공해야 한다. 이러한 사용은 개인 정보가 수집된 목적 또는 이후에 개인이 승인한 목적과 양립할 수 있어야 한다. 또한, 그러한 선택권을 사용하여 고용 기회를 제한하거나 그러한 직원에 대해 징벌적 조치를 취해서는 안 된다.

ii. 일부 EU 회원국으로부터 이전에 대해 일반적으로 적용되는 특정 조건은 EU 외부로 이전된 후에도 해당 정보의 다른 사용을 배제할 수 있으며 이러한 조건은 존중되어야 한다는 점에 유의해야 한다.

iii. 또한 고용주는 직원의 개인 정보 선택 사항을 수용하기 위해 합당한 노력을 기울여야 한다. 예를 들어 여기에는 개인 데이터에 대한 열람 제한, 특정 데이터 익명화 또는 당면한 관리 목적에 실제 이름이 필요하지 않은 경우 코드 또는 가명 할당이 포함될 수 있다.

iv. 승진, 임명 또는 다른 유사한 고용 결정을 함에 있어 조직의 능력에 대한 편견을 피하기 위해 필요한 범위와 기간 동안, 조직은 통지와 선택을 제공할 필요가 없다.

c. 열람 원칙의 적용

i. 열람에 관한 보충 원칙은 인사 관련 맥락에서 요청에 대한 열람을 거부하거나 제한하는 것을 정당화할 수 있는 이유에 대한 지침을 제공한다. 물론, EU의 고용주는 현지 규정을

준수해야 하며, EU 직원들이 데이터 처리 및 저장 위치에 관계없이 본국에서 법률에 의해 요구되는 정보에 열람할 수 있도록 보장해야 한다. EU-U.S. DPF는 미국에서 이러한 데이터를 처리하는 조직이 직접 또는 EU 고용주를 통해 이러한 열람을 제공하는 데 협력할 것을 요구한다.

d. 집행

i. 개인 정보가 고용 관계의 맥락에서만 사용되는 한, 직원에 관한 데이터에 대한 일차적인 책임은 EU에 있는 조직에 있다. 그 결과, 유럽의 직원들이 자신들의 데이터 보호 권리 위반에 대해 불만을 제기하고 내부 검토, 불만 및 항소 절차(또는 노동 조합과의 계약에 따른 해당되는 고충 처리 절차)의 결과에 만족하지 못하는 경우, 직원들이 근무하는 관할 구역의 주 또는 국가 데이터 보호 또는 노동 기관에 전달되어야 한다. 여기에는 개인 정보를 잘못 처리한 것으로 주장된 것이 사용자로부터 정보를 받은 미국 조직의 책임이므로 원칙 위반 혐의가 있는 경우가 포함된다. 이는 데이터 보호법뿐만 아니라 현지 노동법과 노동 협약에 의해 부과되는 종종 중복되는 권리와 의무를 해결하는 가장 효율적인 방법이 될 것이다.

ii. 고용 관계의 맥락에서 EU로부터 이전된 EU 인적 자원 데이터를 사용하고 이러한 이전이 EU-U.S. DPF 내에서 처리되기를 원하는 EU-U.S. DPF에 참여하는 미국 조직은 따라서 이러한 경우에 EU 당국의 조언을 준수하고 조사에 협력할 것을 약속해야 한다.

e. 제3자(역외) 이전 원칙에 대한 책임 적용

i. 항공편 예약, 호텔 객실 예약 또는 보험 적용과 같이 EU-U.S. DPF에 따라 이전된 개인 정보와 관련하여 때때로 참여 기관의 고용 관련된 운영상 필요한 경우, 제3자 이전 책임 원칙에 따라 요구되는 경우와 다르게 열람 원칙의 적용 없이 또는 제3자 컨트롤러와 계약을 체결하지 않고도 소수의 직원의 개인 정보를 컨트롤러에게 이전할 수 있다. 단, 참여 기관이 통지 및 선택 원칙을 준수한 경우에 한한다.

10. 제3자 이전을 위한 의무 계약.

a. 데이터 처리 계약

i. EU에서 미국으로 개인 데이터가 처리 목적으로만 이전되는 경우, EU-U.S. DPF에 대한 프로세서의 참여와 관계없이 계약이 필요하다.

ii. EU 내 데이터 컨트롤러는 단순한 처리를 위한 이전이 이루어졌을 때, 처리 작업이 EU 내에서 이루어졌든 외부에서 이루어졌든 간에, 프로세서가 EU-U.S. DPF에 참여하였는지 관계없이 항상 계약을 체결해야 한다. 계약의 목적은 다음을 확인하기 위함이다:

1. 프로세서가 컨트롤러의 지시에만 따라 행동하도록 한다.

2. 프로세서가 우발적이거나 불법적인 파괴 또는 사고로 인한 손실, 변경, 무단 공개 또는 열람으로부터 개인 데이터를 보호하기 위한 적절한 기술적 및 조직적 조치를 제공하고 제3자 이전이 허용되는지를 이해한다.

3. 처리의 성격을 고려하여 프로세서가 원칙에 따라 권리를 행사하는 개인에 대해 컨트롤러가 대응할 수 있도록 지원한다.

iii. 참여 기관이 적절한 보호를 제공하기 때문에, 그러한 기관과의 단순한 처리를 위한 계약은 사전 승인을 필요로 하지 않는다.

b. 기업의 통제 대상 그룹 내 이전

i. 통제되는 기업 또는 법인 그룹 내의 두 컨트롤러 간에 개인 정보가 이전되는 경우, 제3자 이전에 대한 책임 원칙에 따라 계약이 항상 필요한 것은 아니다. 통제되는 기업 또는 법인 그룹 내의 데이터 컨트롤러는 EU 구속력 있는 기업 규칙(EU Binding Corporate Rules) 또는 기타 그룹 내 도구(예: 규정 준수 및 통제 프로그램)와 같은 다른 도구를 기반으로 이러한 이전을 수행하여 원칙에 따라 개인 정보 보호의 연속성을 보장할 수 있다. 이러한 이전의 경우 참여 조직은 원칙을 준수할 책임이 있다.

c. 컨트롤러 간 이전

i. 컨트롤러 간 이전의 경우 수신자 컨트롤러는 참여 기관이거나 독립적인 청구 메커니즘을 가질 필요가 없다. 참여 조직은 수신자 제3자 컨트롤러와 EU-U.S. DPF에 따라 사용할 수 있는 동일한 수준의 보호를 제공하는 계약을 체결해야 한다(제3자 컨트롤러가 동등한 메커니즘을 제공하는 경우 제3자 컨트롤러가 참여 조직이거나 독립적인 청구 메커니즘을 보유해야 한다는 요건은 제외한다).

11. 분쟁해결 및 집행

a. 청구, 집행 및 책임 원칙은 EU-U.S. DPF 집행을 위한 요건을 규정하고 있다. 원칙의 (a)(ii) 요건을 충족하는 방법은 검증에 관한 보충 원칙에 규정되어 있다. 이 보충 원칙은 (a)(i) 및 (a)(iii)을 다루는데, 두 가지 모두 독립적인 청구 메커니즘을 필요로 한다. 이러한 메커니즘은 다른 형태를 취할 수 있지만 청구, 집행 및 책임 원칙의 요건을 충족해야 한다. 조직은 (i) 원칙을 자체 규칙에 통합하고 청구, 집행 및 책임 원칙에 설명된 유형의 효과적인 집행 메커니즘을 포함하는 민간 부문에서 개발한 개인 정보 보호 프로그램 준수 (ii) 개별 불만 처리 및 분쟁 해결을 제공하는 법적 또는 규제 감독 기관을 준수 또는 (iii) EU에 위치한 DPA 또는 그들의 공식 대리인과 협력하겠다는 약속을 통해 해당 요건을 만족시킨다.

b. 이 목록은 설명을 위한 것이며 제한적이지 않다. 민간 부문은 청구, 집행 및 책임 원칙과 보충 원칙의 요건을 충족하는 한 집행을 제공하기 위한 추가 메커니즘을 설계할 수 있다. 청구, 집행 및 책임 원칙의 요건은 불공정하거나 기만적인 행위를 금지하는 FTC 법 제5조(15 U.S.C. § 45), 항공사 또는 발권 대리인이 항공운송 또는 항공권 판매에서 불공정하거나 기만적인 행위를 하는 것을 금지하는 49 U.S.C. § 41712, 또는 그러한 행위를 금지하는 또 다른 법 또는 규정에 따라 자율 규제 노력을 집행할 수 있어야 한다는 요건에 추가된다.

c. EU-U.S. DPF 약속을 준수하고 프로그램의 관리를 지원하기 위해 조직은 물론 독립적인 청구 메커니즘은 부처가 요청할 경우 EU-U.S. DPF와 관련된 정보를 제공해야 한다. 또한 조직은 DPA에 의해 부처를 통해 언급된 원칙을 준수하는 것에 대한 불만에 신속하게 대응해야 한다. 응답은 불만이 가치가 있는지 여부와, 그렇다면 조직이 문제를 어떻게 해결할 것인지를 다루어야 한다. 부처는 미국의 법률에 따라 수신한 정보의 기밀성을 보호할 것이다.

d. 청구 메커니즘

i. 개인은 독립적인 청구 메커니즘에 의지하기 전에 관련 기관에 불만을 제기할 수 있도록 권장되어야 한다. 조직은 불만을 접수한 후 45일 이내에 개인에게 답변해야 한다. 청구 메커니즘이 독립적인지 여부는 공정성, 투명한 구성 및 자금 조달, 입증된 과거 기록에 의해 특히 입증될 수 있는 사실에 관한 질문이다. 청구, 집행 및 책임 원칙에 의해 요구되는 바와 같이, 개인이 이용할 수 있는 청구는 개인이 쉽게 이용할 수 있고 무료이어야 한다. 독립적인 분쟁 해결 기관은 명백하게 근거가 없거나 경솔하지 않는 한 개인으로부터 받은 각 불만을 조사해야 한다. 이것이 청구 메커니즘을 운영하는 독립 분쟁 해결 기관의 자격 요건의 설정을 배제하는 것은 아니지만, 그러한 요건은 투명하고 정당해야 하며(예를 들어, 프로그램의 범위를 벗어나거나 다른 포럼에서 고려해야 할 불만을 제외하는 것) 정당한 불만을 조사하겠다는 약속을 훼손하는 효과를 가져서는 안 된다. 또한 청구 메커니즘은 불만이 제기될 경우 분쟁 해결 절차가 어떻게 작동하는지에 대한 완전하고 쉽게 이용할 수 있는 정보를 개인에게 제공해야 한다. 그러한 정보는 원칙에 따라 메커니즘의 개인 정보 보호 관행에 대한 통지를 포함해야 한다. 또한 불만 해결 절차를 용이하게 하는 표준 불만 양식과 같은 도구의 개발에 협력해야 한다.

ii. 독립적인 청구 메커니즘은 EU-U.S. DPF에 따라 제공하는 원칙 및 서비스에 관한 정보를 공개 웹 사이트에 포함해야 한다. 이 정보에는 (1) 독립적인 청구 메커니즘에 대한 원칙의 요건에 대한 정보 또는 링크, (2) 부처의 데이터 프라이버시 프레임워크 웹 사이트 링크, (3) EU-U.S. DPF에 따른 분쟁 해결 서비스가 개인에게 무료라는 설명, (4) 원칙 관련 불만 제기 방법에 대한 설명, (5) 원칙 관련 불만의 처리기간 및 (6) 잠재적인 구제 조치 범위에 대한 설명이 포함되어야 한다.

iii. 독립적인 청구 메커니즘은 분쟁 해결 서비스에 관한 종합적인 통계를 제공하는 연례 보고서를 발행해야 한다. 연례 보고서에는 다음이 포함되어야 한다: (1) 보고 연도 동안 접수된 원칙-관련 불만의 총 수 (2) 접수된 불만 유형 (3) 불만을 처리하는 데 걸리는 시간과 같은 분쟁 해결 품질 기준 (4) 접수된 불만 사항의 결과, 특히 부과된 구제 또는 제재의 수와 유형

iv. 부속서 I에 명시된 바와 같이, 중재 옵션은 참여 조직이 해당 개인에 대한 원칙에 따른 의무를 위반했는지 그러한 위반이 완전히 또는 부분적으로 구제되지 않은 상태로 남아 있는지를 잔여 청구(residual claims)에 대해 결정할 수 있도록 개인에게 제공된다. 이 옵션은 이러한 목적에만 이용 가능하다. 예를 들어, 원칙[15]에 대한 예외 또는 EU-U.S. DPF의 적절성에 대한 주장과 관련하여 이 옵션은 이용할 수 없다. 이 중재 옵션에 따라, "EU-U.S. 데이터 프라이버시 프레임워크 패널"(당사자가 합의한 대로 1명 또는 3명의 중재인으로 구성됨)은 개인에 대한 원칙 위반을 구제하는 데 필요한 개인별, 비금전적 및 형평법상 유효한 구제(예를 들어, 해당 개인의 데이터에 대한 열람, 수정, 삭제 또는 반환)를 부과할 권한이 있다. 개인 및 참가 조직은 연방 중재법에 따른 미국법에 따른 중재 결정에 대한 사법적 검토 및 집행을 구할 수 있다.

e. 구제조치 및 제재

[15] 원칙, 개요, para. 5.

i. 독립 분쟁 해결 기관이 제공하는 구제책의 결과에 따라 비준수의 영향이 가능한 한 조직에 의해 취소되거나 수정되어야 하며, 조직에 의한 향후 처리는 원칙에 부합해야 하고, 적절한 경우 불만을 제기한 개인의 개인 데이터 처리가 중단되어야 한다. 제재는 조직이 원칙을 준수하도록 충분히 엄격해야 한다. 다양한 심각도의 다양한 제재를 통해 분쟁 해결 기관은 다양한 수준의 비준수에 적절하게 대응할 수 있다. 제재에는 비준수 결과 공표 및 특정 상황에서 데이터 삭제 요건이 모두 포함되어야 한다.[16] 기타 제재에는 봉인seal 사용 중지 및 제거, 비준수로 인해 발생한 손실에 대한 개인 보상 및 금지 명령(injunctive awards)이 포함될 수 있다. 민간 부문의 독립 분쟁 해결 기관 및 자율-규제 기관은 참여 조직이 판결을 준수하지 않는 사실을 해당 관할권을 가진 정부 기관 또는 법원(적절한 경우) 및 부처에 통지해야 한다.

f. FTC 조치

i. FTC는 상거래에서 불공정하거나 기만적인 행위 또는 관행을 금지하는 FTC법 제5조가 위반되었는지 여부를 결정하기 위해 (i) 프라이버시 자율-규제 기관 및 기타 독립 분쟁 해결 기관, (ii) EU 회원국, (iii) 부처로부터 접수한 원칙 비준수를 주장하는 회부를 우선순위에 기초하여 심의하기로 약속했다. FTC가 제5조가 위반되었다고 믿을 만한 이유가 있다고 판단하는 경우, FTC는 문제가 되는 관행을 금지하는 행정적 정지 명령을 구하거나 연방 지방 법원에 불만을 제기하여 문제를 해결할 수 있으며, 이는 성공하면 동일한 효과의 연방 법원 명령으로 이어질 수 있다. 여기에는 더 이상 데이터 프라이버시 프레임워크 목록에 등재되어 있지 않거나 부처에 대해 자체- 인증을 받은 적이 없는 조직의 원칙 준수 또는 EU-U.S. DPF 참여라는 허위 주장이 포함된다. FTC는 행정적 정지명령 위반에 대해 민사 처벌을 구할 수 있으며 연방 법원 명령 위반에 대해 민사 또는 형사상 모독죄를 구할 수 있다. FTC는 취한 조치를 부처에 통지한다. 부처는 다른 정부 기관이 이러한 회부 또는 원칙 준수 여부를 결정하는 기타 판결의 최종 처분을 부처에 보고할 것을 권장한다.

g. 지속적인 비준수

i. 조직이 지속적으로 원칙을 준수하지 않을 경우, 더 이상 EU-U.S. DPF의 혜택을 받을 자격이 없다. 지속적으로 원칙을 준수하지 못한 조직은 부처에 의해 데이터 프라이버시 프레임워크 목록에서 제거되며 EU-U.S. DPF에 따라 받은 개인 정보를 반환하거나 삭제해야 한다.

ii. 지속적인 비준수는 부처에 대해 자체-인증을 받은 조직이 프라이버시 자율 규제, 독립 분쟁 해결 또는 정부 기관의 최종 결정을 거부하거나, 부처를 포함한 그러한 기관이 조직이 더 이상 신뢰할 수 없을 정도로 원칙을 빈번하게 준수하지 않는다고 결정하는 경우에 발생한다. 부처 이외의 기관에서 그러한 결정을 내린 경우 조직은 그러한 사실을 즉시 부처에 알려야 한다. 그렇게 하지 않을 경우 거짓 진술에 관한 법률(18 U.S.C. § 1001)에 따라 소송이 제기될 수 있다. 조직이 민간 부문 프라이버시 자율 규제 프로그램 또는 독립

[16] 독립 분쟁 해결 기관은 이러한 제재를 사용하는 상황에 대해 재량권을 가진다. 해당 데이터의 민감도는 조직이 원칙을 노골적으로 위반하여 정보를 수집, 사용 또는 공개했는지 여부와 마찬가지로 데이터 삭제가 필요한지 여부를 결정할 때 고려해야 할 요소 중 하나이다.

분쟁 해결 메커니즘에서 탈퇴한다고 해서 원칙 준수 의무가 면제되는 것은 아니며 지속적으로 원칙을 준수하지 않는 것으로 간주된다..

iii. 부서는 조직 자체, 개인 정보 자율 규제 기관 또는 다른 독립 분쟁 해결 기관 또는 정부기관으로부터 그러한 비준수에 대한 통지를 받은 것에 대한 응답을 포함하여 지속적 비준수를 이유로 데이터 프라이버시 프레임워크 목록에서 조직을 제거한다. 그러나 먼저 조직에 30일 전에 통지하고 응답할 기회를 제공한 후에만 가능하다[17]. 따라서 부처에서 관리하는 데이터 프라이버시 프레임워크 목록은 어떤 조직이 EU-U.S. DPF 혜택을 보장받고, 어떤 조직이 더 이상 보장받지 않는지를 명확하게 할 것이다.

iv. EU-U.S. DPF에 대한 재-인증을 목적으로 자율 규제 기구에 참여를 신청하는 조직은 해당 기구에 EU-U.S. DPF에 대한 이전 참여에 대한 모든 정보를 제공해야 한다.

12. 선택 – 옵트 아웃 시기

a. 일반적으로 선택 원칙의 목적은 개인의 기대와 선택에 부합하는 방식으로 개인 정보가 사용되고 공개되도록 보장하는 것이다. 조직이 옵트 아웃을 유효하게 할 시간을 조직에게 부여하는 것과 같이 조직이 설정한 합리적인 제한에 따라 언제든지 다이렉트 마케팅에 개인 정보를 사용하는 "옵트 아웃" 선택권을 행사할 수 있어야 한다. 조직은 또한 "옵트 아웃"을 요청하는 개인의 신원을 확인하기 위해 충분한 정보를 요구할 수 있다. 미국에서는 개인이 중앙 "옵트 아웃" 프로그램을 사용하여 이 옵션을 행사할 수 있다. 어쨌든 개인은 이 옵션을 행사할 수 있고 쉽게 사용할 수 있고 저렴한 메커니즘을 제공받아야 한다.

b. 마찬가지로, 조직이 개인에게 더 이상의 직접 마케팅 커뮤니케이션 수신을 거부할 수 있는 기회를 즉시 제공하고 조직이 개인의 의사를 따른다면, 조직이 정보를 사용하기 전에 옵트 아웃 기회를 개인에게 제공할 수 없을 때, 조직은 특정 직접 마케팅 목적을 위해 정보를 사용할 수 있다.

13. 여행 정보

a. 상용 고객 우대 프로그램 또는 호텔 예약 정보 등 항공사 승객 예약 및 기타 여행 정보, 종교적 요구 사항 또는 신체적 지원을 충족하기 위한 식사와 같은 특별 처리 요구 사항은 여러 가지 상황에서 EU 외부에 위치한 조직으로 이전될 수 있다. GDPR에 따라 개인 데이터는 적절한 결정이 없는 경우 GDPR 제46조에 따라 적절한 데이터 보호 안전장치가 제공되거나 특정 상황에서 GDPR 제49조의 조건 중 하나가 충족되는 경우(예를 들어, 데이터 주체가 이전에 대해 명시적으로 동의한 경우) 제3국으로 이전될 수 있다. EU-U.S. DPF에 가입한 미국 조직은 개인 데이터에 대한 적절한 보호를 제공하므로 GDPR 제46조에 따라 이전 수단을 마련하거나 GDPR 제49조의 조건을 충족하지 않고도 GDPR 제45조에 따라 EU로부터 데이터 이전을 받을 수 있다. EU-U.S. DPF에는 민감한 정보에 대한 특정 규칙이 포함되어 있으며, 이러한 정보(예: 신체적 지원에 대한 고객의 요구 사항과 관련하여 수집해야 할 수 있는 정보)는 참여 조직으로의 이전에 포함될 수 있다. 그러나 모든 경우에 정보를 이전하는 조직은 자신이 활동하는 EU 회원국(특히, 민감한 데이터 처리에 대한 특별 조건을 부과할 수 있는 회원국)의

[17] 부처는 통지에 조직이 통지에 응답해야 하는 기간(반드시 30일 미만임)을 표시한다.

법률을 준수해야 한다.

14. 제약 및 의료 제품

a. EU/회원국 법률 또는 원칙의 적용

i. 개인 데이터 수집 및 미국으로의 이전 전에 발생하는 모든 처리에 EU/회원국 법률이 적용된다. 원칙은 일단 데이터가 미국으로 이전되면 해당 데이터에 적용된다. 의약품 연구 및 기타 목적으로 사용되는 데이터는 적절한 경우 익명으로 처리되어야 한다.

b. 미래 과학적 연구

i. 특정 의학 또는 약학 연구에서 개발된 개인 데이터는 종종 미래의 과학 연구에서 중요한 역할을 한다. 하나의 연구를 위해 수집된 개인 데이터가 EU-U.S. DPF에 속한 미국 조직으로 이전되는 경우, 처음에 적절한 통지 및 선택이 제공된 경우 조직은 새로운 과학 연구 활동을 위해 데이터를 사용할 수 있다. 이러한 통지는 정기적인 후속 조치, 관련 연구 또는 마케팅과 같은 데이터의 향후 특정 사용에 대한 정보를 제공해야 한다.

ii. 원본 데이터에 대한 새로운 통찰력, 새로운 의학적 발견과 발전, 공중 보건 및 규제 개발로 인해 새로운 연구 용도가 발생할 수 있기 때문에 데이터의 모든 미래 사용을 명시할 수는 없다. 따라서 적절한 경우, 통지에는 개인 데이터가 예상치 못한 미래의 의료 및 제약 연구 활동에 사용될 수 있다는 설명이 포함되어야 한다. 사용이 개인 데이터가 원래 수집되었거나 개인이 후속적으로 동의한 일반적인 연구 목적과 일치하지 않는 경우, 새로운 동의를 받아야 한다.

c. 임상 시험에서 탈퇴

i. 참가자는 언제든지 임상 시험에서 탈퇴를 결정하거나 요청 받을 수 있다. 탈퇴 이전에 수집된 모든 개인 데이터는 임상 시험의 일부로 수집된 다른 데이터와 함께 여전히 처리될 수 있지만, 참여에 동의한 시점에 통지를 통해 참가자에게 이를 분명히 밝힌 경우에 한한다.

d. 규제 및 감독 목적을 위한 이전

i. 제약 및 의료 기기 회사는 규제 및 감독 목적으로 EU에서 수행된 임상 시험의 개인 데이터를 미국의 규제 기관에 제공할 수 있다. 통지 및 선택의 원칙에 따라 회사 소재지 및 기타 연구원 정보 등은 규제 기관 이외의 당사자에게 유사한 이전이 허용된다.

e. "눈가림(blinded)" 연구

i. 많은 임상 시험에서 객관성을 보장하기 위해 참가자와 종종 조사자도 각 참가자가 받을 수 있는 치료에 대한 정보를 열람할 수 없다. 그러한 정보를 열람할 경우 연구 조사 및 결과의 유효성이 위태로워질 수 있다. 그러한 임상 시험("눈가림" 연구라고 함)의 참가자는 참가자가 임상시험에 참가할 때 이러한 제한사항이 설명되었고 그러한 정보의 공개가 연구 활동의 무결성을 위태롭게 할 경우, 시험 중에 그들의 치료에 대한 데이터 열람이 제공될 필요가 없다.

ii. 이러한 조건 하에서 임상시험에 참여하기로 동의하는 것은 열람권을 합리적으로 포기하는 것이다. 임상시험 종료 및 결과 분석 후 참가자는 요청 시 데이터를 열람할 수 있어야 한다.

참가자들은 1차적으로 임상 시험 내에서 치료를 받은 의사 또는 기타 의료 서비스 제공자에게 요청하거나 2차적으로 후원 조직(제약회사)에 이를 요청해야 한다.

f. 제품 안전성 및 효능 모니터링

i. 제약 회사 또는 의료기기 회사는 이상사례 보고 및 특정 의약품 또는 의료기기를 사용하는 환자/대상자의 추적을 포함한 제품 안전 및 효능 모니터링 활동에서 통지, 선택, 제3자 이전에 대한 책임 및 열람 원칙과 관련하여 규제 요건 준수를 방해하는 범위까지 원칙을 적용할 필요가 없다. 이는 예를 들어 제약 및 의료기기 회사에 대한 의료 제공자의 보고서와 식품의약국과 같은 정부 기관에 대한 제약 및 의료기기 회사의 보고서와 관련하여 모두 사실이다.

g. 키-코드화 된 데이터

i. 항상, 연구 데이터는 개별 데이터 주체의 신원이 드러나지 않도록 주요 조사자에 의해 고유하게 원천지에서 키- 코드화 된다. 이러한 연구를 후원하는 제약 회사는 키를 받지 않는다. 고유 키 코드는 연구자만이 보유하므로, 이들만이 특별한 상황에서(예: 후속 치료가 필요한 경우) 연구 대상자를 식별할 수 있다. EU 법에 따라 EU 개인 데이터를 이러한 방식으로 코딩하여 EU에서 미국으로의 해당 데이터 이전에는 원칙이 적용된다.

15. 공공 기록 및 공개적으로 이용 가능한 정보

a. 조직은 공개된 출처의 개인 데이터에 보안, 데이터 무결성 및 목적 제한 원칙, 그리고 청구, 집행 및 책임 원칙을 적용해야 한다. 이 원칙들은 공공 기록(즉, 정부 기관 또는 기업이 보유한 것으로 일반 대중의 협의에 공개되는 모든 수준의 기록)에서 수집된 개인 데이터에도 적용된다.

b. 비공개 기록 정보와 결합되지 않고 관련 관할권에서 설정한 협의 조건이 존중되는 한 공개 기록 정보에 통지, 선택 또는 제3자 이전에 대한 책임 원칙을 적용할 필요가 없다. 또한 유럽 양도자가 그러한 정보가 해당 조직이 의도하는 용도에 대해 해당 원칙의 적용을 요구하는 제한의 대상임을 표시하지 않는 한, 공개적으로 사용 가능한 정보에 통지, 선택 또는 제3자 이전 책임 원칙을 적용할 필요가 일반적으로 없다. 조직은 게시된 자료에서 그러한 정보를 얻는 사람들이 그러한 정보를 사용하는 방법에 대해 책임을 지지 않는다.

c. 조직이 의도적으로 원칙을 위반하여 개인 정보를 공개하여 자신이나 다른 사람이 이러한 예외의 혜택을 받을 수 있는 것으로 밝혀지면, 해당 조직은 EU-U.S. DPF의 혜택을 받을 자격을 상실한다.

d. 공개 기록 정보가 다른 개인 정보(공개 기록 정보에 대한 색인을 작성하거나 정리하는 데 사용되는 소량은 제외) 와 결합되지 않는 한 공개 기록 정보에 열람 원칙을 적용할 필요는 없지만, 관련 관할권이 설정한 모든 협의 조건은 존중되어야 한다. 이와 대조적으로, 공개 기록 정보가 다른 비공개 기록 정보와 결합되는 경우(위에서 특별히 언급한 것 이외), 조직은 허용된 다른 예외의 적용을 받지 않는다고 가정하고, 그러한 모든 정보에 대한 열람을 제공해야 한다.

e. 공공 기록 정보와 마찬가지로, 비공개 정보와 결합되지 않는 한 이미 일반 대중에게 공개된

정보에 대한 열람을 제공할 필요는 없다. 공개적으로 사용 가능한 정보를 판매하는 사업을 하는 조직은 열람 요청에 대한 응답으로 조직의 관례에 따른 수수료를 청구할 수 있다. 또는 개인이 원래 데이터를 편집한 조직에 자신의 정보에 대한 열람 권한을 요청할 수 있다.

16. 공공 기관의 열람 요청

a. 개인정보 열람에 대한 공공기관의 합법적인 요청과 관련하여, 투명성을 제공하기 위해 참여 조직은 법 집행 또는 국가 안보상의 이유로 공공기관으로부터 받은 개인 정보 요청 건수에 대해 준거법에 따라 이러한 공개가 허용되는 범위 내에서 정기적인 투명성 보고서를 발행할 수 있다.

b. 정보 커뮤니티에 의해 공개된 정보와 함께 참여 조직이 이 보고서들에 제공한 정보는 다른 정보와 함께 원칙에 따라 EU-U.S. DPF의 기능에 대한 정기적인 공동 검토에 정보를 제공하기 위해 사용될 수 있다.

c. 통지 원칙의 (a)(xii)에 따른 통지의 부재는 합법적인 요청에 대응하는 조직의 능력을 방해하거나 손상시키지 않는다.

부속서 I: 중재 모델

본 부속서 I은 EU-U.S. DPF에 참여하는 조직이 청구, 집행 및 책임 원칙에 따라 청구를 중재할 의무가 있는 조건을 제공한다. 아래에 설명된 구속력 있는 중재 옵션은 EU-U.S. DPF의 적용을 받는 데이터에 관한 특정 "잔여(residual)" 청구에 적용된다. 이 옵션의 목적은 다른 EU-U.S. DPF 메커니즘에 의해 해결되지 않은 원칙 위반 청구를 해결하기 위해 개인의 선택에 따라 신속하고 독립적이며 공정한 메커니즘을 제공하는 것이다.

A. 범위

잔여 청구에 대해, 참여 조직이 해당 개인에 대한 원칙에 따른 의무를 위반했는지 및 그러한 위반이 완전히 또는 부분적으로 미해결 상태로 남아 있는지를 결정하도록 개인에게 이 중재 옵션이 제공된다. 이 옵션은 이러한 목적에 대해서만 사용할 수 있다. 예를 들어, 원칙[18]에 대한 예외 또는 EU-U.S. DPF의 적절성에 대한 주장과 관련하여 이 옵션은 사용할 수 없다.

B. 가능한 구제책

이러한 중재 옵션에 따라 "EU-U.S. 데이터 프라이버시 프레임워크 패널"(당사자들이 합의한 대로, 1명 또는 3명의 중재자로 구성된 중재 패널)은 오직 개인과 관련하여 원칙 위반을 시정하는 데 필요한 개인별, 비금전적, 공평한 구제책(예: 해당 개인의 데이터에 대한 열람, 수정, 삭제, 또는 반환)을 부과할 권한이 있다. 이러한 것들은 구제 수단과 관련하여 EU-U.S. 데이터 프라이버시 프레임워크 패널의 유일한 권한이다. 구제 수단을 고려할 때 EU-U.S. 데이터 프라이버시 프레임워크 패널은 EU-U.S. DPF에 따라 다른 메커니즘에 의해 이미 부과된 다른 구제 수단을 고려해야 한다. 손해 배상금, 비용, 수수료 또는 다른 구제 수단은 이용할 수 없다. 각 당사자는 자신의 변호사 비용을 부담한다.

C. 사전-중재 요건

이 중재 옵션을 실행하기로 결정한 개인은 중재 청구를 시작하기 전에 다음 단계를 수행해야 한다. (1) 청구된 위반 사항을 조직에 직접 제기하고, 조직에 분쟁 해결 및 집행에 관한 보충 원칙의 섹션 (d)(i)에 명시된 기간 내에 문제를 해결할 수 있는 기회를 제공한다. (2) 개인에게 비용을 부담시키지 않고 원칙에 따른 독립적인 청구 메커니즘을 활용한다. (3) 개인의 DPA를 통해 부처에 문제를 제기하고 부처가 개인에게 비용을 부담하지 않고 부처의 국제무역청이 보낸 서한에 명시된 기간 내에 문제를 해결하기 위해 최선의 노력을 기울일 수 있는 기회를 제공한다.

이 중재 옵션은, 원칙 위반에 대한 개인의 동일한 청구가 (1) 이전에 구속력 있는 중재의 대상이 된 경우, (2) 개인이 당사자인 법원 소송의 최종 판결의 대상인 경우, 또는 (3) 당사자들에 의해 이전에 해결된 경우, 발동되지 않을 수 있다. 또한, DPA가 (1) 데이터 보호 당국의 역할에 대한 보충 원칙 또는 인적 자원 데이터에 대한 보충 원칙에 따라 권한을 가진 경우, 또는 (2) 청구된 위반을 조직과 직접 해결할 수 있는 권한을 가진 경우, 이 옵션은 발동되지 않을 수 있다. EU 데이터 컨트롤러에 대한 동일한 청구를 해결할 수 있는 DPA의 권한만으로는 DPA 권한에 구속되지 않는 다른 법인에 대한 이 중재 옵션의 발동이 배제되지 않는다.

D. 결정의 구속성

이 구속력 있는 중재 옵션을 적용하는 개인의 결정은 전적으로 자발적이다. 중재 결정은 중재의 모든 당사자에게 구속력을 갖는다. 일단 개시되면 개인은 다른 포럼에서 동일한 청구 위반에 대한 구제를 요청할 수 있는 옵션을 포기하는 것이 된다. 단, 비금전적 형평적 구제가 청구된 위반을 완전히 구제하지 않는 경우 개인의

[18] 원칙, 개요, para. 5.

중재 발동은 법원에서의 손해배상 청구를 막지 않을 것이다.

E. 심사 및 집행

개인 및 참여 조직은 연방 중재법(Federal Arbitration Act)하의 미국 법률에 따라 중재 결정에 대한 사법적 심사 및 집행을 요청할 수 있다.[19] 그러한 사건은 그 관할 지역이 참여 조직의 주요 사업장을 포함하는 연방지방법원에 제기되어야 한다.

이 중재 옵션은 개별 분쟁을 해결하기 위한 것이며, 중재 결정은 향후 중재, EU 또는 미국 법원 또는 FTC 소송 절차를 포함하여 다른 당사자와 관련된 문제에서 설득력이 있거나 구속력 있는 선례 역할을 하기 위한 것이 아니다.

F. 중재 패널

당사자들은 아래에서 논의된 중재자 목록에서 EU-U.S. 데이터 프라이버시 프레임워크 패널의 중재자를 선정한다.

준거법에 따라, 부처와 위원회는 독립성, 무결성 및 전문성에 기초하여 선정된 최소 10명의 중재자 목록을 개발할 것이다. 이 절차와 관련하여 다음이 적용되어야 한다:

중재자는:

(1) 예외적인 상황이나 귀책 사유로 인해 제거되지 않는 한 3년 동안 명단에 남게 되며, 위원회에 사전 통지하여 부처가 추가 3년 기간으로 갱신할 수 있다.

(2) 당사자, 참여 조직, 미국, EU, EU 회원국 또는 기타 정부 기관, 공공 기관 또는 집행 기관의 지시를 받거나 이들과 제휴해서는 안 된다.

(3) 미국에서 법률 업무를 수행할 수 있고 EU 데이터 보호법에 대한 전문 지식을 갖춘 미국 개인정보 보호법

---

[19] 연방중재법("FAA") 제2장은 "[FAA 섹션 2]에 기술된 거래, 계약 또는 협약을 포함하여 계약 여부에 관계없이 상업적으로 간주되는 법적 관계에서 발생하는 중재 합의 또는 중재 판정은 [1958년 6월 10일자 외국 중재 판정의 인정 및 집행에 관한 협약의 적용을 받는다. 21 U.S. T. 2519, T.I.A.S. 6997호 ("뉴욕협약")]"라고 규정한다. 9 U.S.C. § 202. FAA는 또한 "전적으로 미국 시민들 간의 그러한 관계로부터 발생하는 합의 또는 판정은 그 관계가 해외에 위치한 재산을 포함하거나, 해외에서 수행 또는 집행을 예상하거나, 하나 이상의 외국 국가와 다른 합리적인 관계를 갖지 않는 한 [뉴욕] 협약에 해당하지 않는 것으로 간주된다."라고 규정한다. *Id.* 2장에 따라, "중재 당사자는 이 장에 따라 관할권이 있는 법원에 다른 중재 당사자에 대해 판정을 확인하는 명령을 신청할 수 있다. 법원은 상기 [뉴욕] 협약에 명시된 판정의 승인 또는 집행을 거부하거나 연기하는 근거를 발견하지 않는 한 해당 판정을 확인해야 한다." *Id.* § 207. 제2장은 또한 "미국 지방 법원은.... 논란이 되고 있는 금액에 관계없이 [뉴욕 협약에 따른] 소송 또는 절차에 대해 원래의 관할권을 가질 것이다."라고 추가로 규정한다 *Id.* § 203.

2장은 또한 "1장은 이 장(챕터) 또는 미국이 비준한 [뉴욕] 협약과 충돌하지 않는 범위 내에서 이 장에 의거하여 제기된 소송 및 절차에 적용된다"고 규정하고 있다 *Id.* § 208. 이에 따라, 제1장은 다음과 같이 규정한다. "이후에 그러한 계약이나 거래 또는 거래의 전체 또는 일부에 대한 이행 거부로 인해 발생하는 분쟁을 중재에 의해 해결하기 위해 상거래를 포함하는 거래를 증명하는 계약의 서면 조항, 또는 그러한 계약, 거래 또는 거부로 인해 발생하는 기존 분쟁을 중재에 회부하기 한 서면 합의는 유효하고, 취소불가하며, 집행 가능하다. 단 계약 취소에 대한 법률 또는 형평법상 존재하는 근거가 있는 경우는 제외한다." *Id.* § 2. 1장은 또한 다음과 같이 규정한다. "모든 중재 당사자는 판정을 확인하는 명령을 지정된 법원에 신청할 수 있으며, 그에 따라 법원은 [FAA]의 섹션 10 및 11에 규정된 대로 해당 판정이 무효화되거나 변경되거나 또는 수정되지 않는 한 그러한 명령을 승인해야 한다." *Id.* § 9.

전문가여야 한다.

G. 중재 절차

해당 부처와 위원회는 준거법에 따라 "EU-U.S. 데이터 프라이버시 프레임워크 패널"의 절차를 규율하는 중재 규칙을 채택하는 데 동의했다.[20] 절차를 규율하는 규칙을 변경해야 하는 경우 부처와 위원회는 해당 규칙을 개정하거나 다음 각 고려 사항에 따라 적절하게 기존의 확립된 다른 미국 중재 절차들을 채택하는 데 동의한다:

1. 개인은 위의 사전-중재 요건 조항에 따라 조직에 "통지"를 전달하여 구속력 있는 중재를 개시할 수 있다. 통지에는 청구를 해결하기 위해 C항에 따라 취한 조치의 요약, 주장된 위반에 대한 설명, 개인의 선택에 따라 주장된 청구와 관련된 모든 증빙 문서 및 자료 및/또는 법률에 대한 논의가 포함되어야 한다.
2. 개인의 동일한 청구 위반이 중복 구제 또는 절차를 받지 않도록 보장하기 위한 절차가 개발될 것이다.
3. FTC 조치는 중재와 병행하여 진행될 수 있다.
4. 미국, EU 또는 기타 EU 회원국의 대표자나 기타 정부 기관, 공공 기관 또는 집행 기관은 이러한 중재에 참여할 수 없다. 단, EU 개인의 요청이 있을 경우 DPA는 통지의 작성에 대해서만 도움을 제공할 수 있지만 DPA는 이러한 중재와 관련된 개시(discovery) 또는 기타 자료에 접근할 수 없다.
5. 중재 장소는 미국이며, 개인은 비디오 또는 전화 참여를 선택할 수 있으며, 이는 개인에게 무료로 제공될 것이다. 직접 참여는 필요하지 않을 것이다.
6. 중재의 언어는 당사자가 달리 합의하지 않는 한 영어를 사용한다. 합리적인 요청에 따라 개인이 변호사에 의해 대리되는지 여부를 고려하여 중재 청문회에서의 해석뿐만 아니라 중재 자료의 번역도 개인에게 무료로 제공된다. 단, EU-U.S. 데이터 프라이버시 프레임워크 패널이 특정 중재 상황에서 이것이 정당하지 않거나 불합리한 비용 발생으로 이어질 수 있다고 판단하지 않는 경우에 한한다.
7. 중재인에게 제출된 자료는 기밀로 취급되며 중재와 관련해서만 사용된다.
8. 필요한 경우 개인별 개시(discovery)가 허용될 수 있으며, 이러한 개시는 당사자들에 의해 기밀로 처리되며 중재와 관련하여만 사용된다.
9. 중재는 당사자들이 별도로 합의하지 않는 한 문제가 발생한 조직에 통지가 전달된 후 90일 이내에 완료되어야 한다.

H. 비용

중재인은 중재 비용이나 수수료를 최소화하기 위해 합리적인 조치를 취해야 한다.

해당 부처는, 준거법에 따라, 중재자 수수료를 포함한 중재 비용을 최대 한도("한도cap")까지 충당하기 위한 것으로 조직의 규모에 기초하여 참가 조직이 기여하는 기금의 유지 관리를 용이하게 한다. 기금은 제3자에 의해 관리되며, 제3자는 기금 운영에 대해 부처에 정기적으로 보고한다. 부처는 제3자와 협력하여 기여금 또는 중재 비용 상한액 조정의 필요성을 포함하여 기금의 운영을 주기적으로 검토하며, 무엇보다도 참여 조직에

[20] 미국중재협회("AAA")의 국제 부서인 국제분쟁해결센터("ICDR")(집단적으로 "ICDR-AAA"라 한다)는 원칙 부속서 I에 따라 중재를 관리하고 확인된 중재 기금을 관리하기 위해 부처에 의해 선정되었다. 2017년 9월 15일, 부처와 위원회는 원칙 부속서 I에 설명된 구속력 있는 중재 절차와 상업 중재인에 대해 일반적으로 받아들여지는 윤리적 표준 및 원칙 부속서 I에 부합하는 중재인 행동 강령을 채택하기로 합의했다. 부처와 위원회는 중재 규칙과 행동 강령을 EU-U.S. DPF에 따른 업데이트를 반영하도록 조정하기로 합의했으며, 부처는 ICDR-AAA와 협력하여 이러한 업데이트를 수행할 것이다.

과도한 재정적 부담이 부과되지 않을 것이라는 이해와 함께, 중재 횟수와 중재 비용 및 중재 시간을 고려할 것이다. 부처는 제3자와 함께 한 그러한 검토의 결과를 위원회에 통지할 것이며, 위원회에 기여금 금액 조정에 대한 사전 통지를 제공할 것이다.

변호사 비용은 이 조항 또는 이 조항에 따른 기금에 의해 충당되지 않는다.