

EU 진출 기업을 위한 유럽 일반 개인정보 보호규정(GDPR) 핸드북



kotra

대한무역투자진흥공사



EU 진출 기업을 위한 유럽 일반 개인정보 보호규정(GDPR) 핸드북

Korean



kotra

대한무역투자진흥공사

〈일러두기〉

본 핸드북은 유럽 일반 개인정보 보호규정(GDPR) 준수를 위한 우리 기업들의 조치사항을 요점별로 정리하여 참고용으로 제공하는 것이며, 내용의 일부 또는 전체로 인하여 발생 가능한 모든 결과에 대하여 일체의 책임이 없음을 밝힙니다.

아울러, 영문 원문은 국제 법무 법인 Taylor Wessing의 GDPR 전문 독일 법률팀에서 제공하였고, 원문에 충실한 번역을 위하여 한국인터넷진흥원(KISA)의 번역 감수를 협조 받았습니다. 다만, 원문을 한글로 번역하는 과정에서 오역의 발생 가능성을 배제할 수 없는 바, 오해의 소지가 있을 경우 원문을 참고하시기 바랍니다.

- 최근, 영국의 개인정보 관리감독기구(ICO)는 해킹에 의한 개인정보 유출에 따른 GDPR 위반으로 BA(British Airways)에 204백만 유로 (한화 2,700억원) 과징금 부과 계획 발표 (' 19.07.)
- GDPR 시행 이후 첫 9개월이 지난 시점까지는 과징금 부여 금액 총계가 56백만 유로 육박, 그 중 2019년 1월 프랑스 구글 50백만 유로(한화 642억 원) 건이 가장 높은 부과금 기록

GDPR 발효에 따른 유럽의 개인정보 보호 시스템 이해를 위한 핸드북

GDPR은 EU 일반 개인정보 보호 규정으로(EU General Data Protection Regulation)으로, 2018년 5월 25일에 발효되어 유럽 전역에서 적용되고 있는 개인정보 보호 규정이다. EU 역내외에서 활동 중인 많은 한국 기업은 일상적인 업무 수행에서 이미 GDPR을 직면하고 있다.

그러나 아직도 많은 한국 기업이 GDPR에 대해 의문을 품은채 그 정체에 대해서는 잘 알지 못하고 있는 상황이다. EU의 규정(regulation)인 GDPR이 무엇인지부터 해서, 이 규정이 현지 업무 수행에 어떠한 영향을 미치는지에 대한 의문이 난무하다.

이런 질문은 모두 넓은 범위의 GDPR에 관련된다. 첫째, GDPR은 유럽 법률에서 매우 폭넓게 정의하는 개인정보(personal data) 처리와 관련하여 자연인(즉, 정보주체)을 포괄적으로 보호하는 규칙을 규정한다. 둘째, GDPR은 EU 내 거의 모든 민간 및 공공 부문 조직에서 발생하는 개인정보 처리에 적용된다. EU 역외의 조직도 EU 주민의 개인정보를 처리하는 경우에는 GDPR이 적용된다.

GDPR의 핵심은 책임성이다. 즉 조직은 개인정보 처리 활동에 대한 GDPR의 요구사항을 파악하고 GDPR을 준수할 수 있는 시스템과 메커니즘을 구현하였다는 것을 언제든지 입증할 수 있어야 한다.

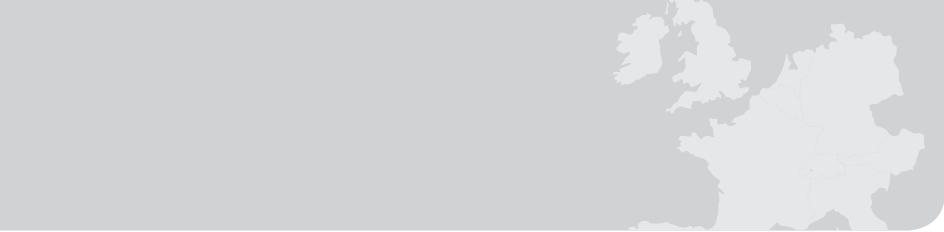
GDPR을 준수하게 하고자, EU는 위반에 대한 최대 과징금을 2,000만 유로 또는 해당 회사 그룹 전 세계 매출액의 4% 중 더 많은 금액으로 부과하도록 인상하였다.

이러한 이유로 GDPR은 여전히 많은 주목을 받고 있다.

따라서 EU 내에 있는 조직뿐만 아니라, EU 내에 조직이 없더라도 EU 내에서 사업을 하는 모든 조직은, 자신이 GDPR의 적용 대상인지를 평가하고 적시에 조치를 취하는 것이 중요하다.

CONTENTS

| | |
|---|-----------|
| I. 핸드북 구성 | 8 |
| 1. 사전에 참고하세요 | 8 |
| 2. GDPR 준수를 위한 기초 | 9 |
| II. 12가지 핵심 사항 | 10 |
| III. GDPR 전문용어 정리 | 12 |
| IV. GDPR 준수를 위한 조치사항은 무엇인가? | 16 |
| 1. GDPR의 적용 범위는 어디까지인가? | 16 |
| 1.1 우리 기업은 대개인정보를 취급하는가? | 17 |
| 1.2 GDPR의 지리적 적용 범위는 어떻게 되는가? | 21 |
| 1.3 GDPR에서 말하는 개인정보란 무엇인가? | 22 |
| 2. 개인정보의 적절한 처리절차 | 28 |
| 2.1. 일반적인 개인정보 취급 시 | 29 |
| 2.2 개인정보 중에서도 민감정보 취급 시 | 38 |
| 3. 개인정보 취급 시 유의해야 할 기본 수칙 | 40 |
| 3.1 개인정보 처리 절차에 대한 투명성 보장 | 41 |
| 3.2 개인정보에 한 활용 목적의 제한 및 관련 처리 절차의 최소화 | 43 |
| 3.3 개인정보의 정확성 보장 | 45 |
| 3.4 개인정보의 보유 기간 제한 | 45 |
| 3.5 개인정보의 무결성 및 기밀성 보장 | 46 |
| 3.6 개인정보 보호 적용 설계 및 보호 기본 설정 | 47 |
| 3.7 개인정보 보호 영향 평가(PIA) | 47 |
| 4. 정보주체의 권리 보장을 위한 우리 기업의 조치사항은 무엇인가? | 50 |
| 4.1 열람권(Right to Access) 보장 | 50 |
| 4.2 삭제권, 정정권, 제한권 보장 | 51 |



- 4.3 이동권(Right to Data Portability) 보장52
- 4.4 반대권(Right to Object) 보장53
- 5. 기업의 책임성은 무엇이며, 문서화 요건은 어떻게 충족시키는가?54
- 6. 기술적·관리적 조치(Technical and Organisational Measure)는 어디까지? ...56
 - 7. 개인정보 보호 책임자(DPO) 선임이 필요한 경우는 언제인가?58
 - 7.1 개인정보 보호 책임자의 역할58
 - 7.2 개인정보 보호 책임자 지정 의무가 있는 기업 유형58
- 8. 개인정보의 EU 국외 이전 등 제3자에게 제공하는 경우59
 - 8.1. 그룹 내부에서 이전하는 경우60
 - 8.2. 프로세서에게 이전하는 경우60
 - 8.3. EU/EEA 국역외로 이전하는 경우61
- 9. GDPR의 법적 구속력62
- 10. 감독기구와 협력64
- 11. 개인정보 침해 시 대응 조치65
- 12. GDPR 준수를 입증하는 방법67

V. 진출 기업의 업무 유형별 대응사례 제시 68

- 1. 웹사이트 및 앱을 운영하는 경우68
- 2. 현지직원의 개인정보 처리절차.....71
- 3. 마케팅을 수행하는 경우.....73
- 4. 빅데이터를 활용하는 경우.....75
- 5. 사물인터넷(Internet of Things)을 활용하는 경우.....76
- 6. 의료 서비스를 제공하는 경우77

VI. 단계별 가이드(Step-by-Step Guide) 80

VII. GDPR에 대한 추가 정보 및 관련 출처 82

I 핸드북 구성

1 사전에 참고하세요

개인정보 보호(Data Protection)는 결코 쉬운 주제가 아니며, 이를 이해하기 위해서는 GDPR의 특정 용어와 개인정보 처리 원칙을 먼저 숙지해야 한다.

본 안내서는 GDPR을 준수하기 위해 기업이 취해야하는 조치를 개략적으로 설명하고 GDPR로 인해 발생하는 주요 도전 과제에 관한 정보를 제공하기 위해 작성되었다.

본 안내서가 기업이 GDPR을 준수하거나 최소한 GDPR을 더 잘 이해하는 데 도움이 되기를 기대한다.

본 안내서가 포함하고 있는 내용은 GDPR에 근거한 개인정보 취급 지침이며 권고 사항이라는 것을 유념해야 한다. 본 안내서는 법적 구속력이나 강제력이 있는 규칙을 규정하지는 않는다. 해당 국가의 법률이나 규정이 특정 측면과 관련하여 추가 요건이나 더 엄격한 요건을 규정하는 경우, 언제든지 이 지침을 대체할 수 있다.

또한 본 안내서의 내용은 GDPR에 대한 포괄적인 개요를 제공하지만, 국가 법률에 대한 적절한 법적 자문을 대체할 수는 없다. 본 안내서가 GDPR 준수를 위한 좋은 가이드이며, 안내서의 내용이 국가의 법률을 준수하는 경우, 안내서의 개인정보 처리 원칙을 따를 것을 강력하게 권장한다.

2 GDPR 준수를 위한 기초

GDPR을 이해하기 위해서는 다음 내용을 숙지해야 한다.

1. 기업에 GDPR이 적용되는지 여부와, 적용된다면 적용되는 이유를 이해한다.
2. GDPR의 목적과 기본적인 개인정보 처리 원칙을 이해한다.
3. 우선 조치 수단을 이해하고 적용한다.
4. 기업이 처한 상황을 이해하기 위한 체크리스트를 사용한다.

이런 주제를 숙지한 후 더 포괄적인 접근법을 원하는 경우, 안내서 마지막 장에서 설명하는 단계별 지침(Step-by-Step Guide)을 따르면 된다. 단, 모든 상황에 적용할 수 있는 해법은 없다는 점과 해법은 개별 사안에 따라 달라진다는 점을 명심해야 한다. 이 과정을 마친 후에는 GDPR 준수를 위한 프로젝트를 시작할 수 있으며,

5. 다른 필수 보호조치(safeguard)를 실시할 수 있다.
6. 기업이 취하는 개인정보 보호 수단의 효과성을 유지하고 이를 정기적으로 점검하며, 현재의 진행 사항을 고려하여 지속적으로 개선한다.

관련 법률이 빠르게 발전하고 있기 때문에, GDPR 준수는 반복적이며 계속 진행 중인 과정이다. 따라서 GDPR을 준수하는 것이 모든 것을 해결하는 절차가 아니며 끊임없이 주의를 기울여야 한다는 점을 인지해야 한다.



II 12가지 핵심 사항

"GDPR과 관련해서 알아야 하는 가장 중요한 사항은 무엇인가?"라는 질문에 대한 답, 몇 가지 진술과 제안으로는 GDPR을 정의할 수 없다는 것이다. 그러나 본 안내서에서는 다음의 12개 핵심 사항을 기억하길 권장한다.

1. **GDPR의 지리적 적용 범위는 매우 광범위하다!** EU시민이나 EU 역내에 있는 사람의 개인정보를 처리하는 경우, 대부분 GDPR이 적용될 것이다.
2. **(거의) 모든 것이 개인정보이다!** 개인정보인지 여부가 확실하지 않은 정보는 대부분 개인정보이다! 익명처리된 정보는 매우 드물다.
3. **적법한 이유가 없는 경우, 개인정보 처리는 모두 금지된다.** 개인정보 처리 시 GDPR이 준수되는지를 보장하기 위해서는 구체적 법률 조항, 명시적 동의가 있거나 개인정보 처리자의 구체적이고 적법한 이익을 위해서여야 한다. 후자의 경우, 다소 엄격하게 해석한다.
4. **민감정보(special categories of personal data)에는 특별한 규정이 적용된다.** 예를 들어 건강 관련된 개인정보를 처리하는 경우, 충족하기 매우 어려운 추가 요건이 적용될 수 있다. 따라서 이런 종류의 개인정보를 다루는 일은 상당히 복잡할 수 있으며, 매우 면밀한 점검이 요구된다.
5. **책임성 - 모든 것을 입증할 수 있어야 한다!** 책임성은 새로운 개념이지만 다른 개념보다 더 중요한 것으로 보인다. 유럽 내 감독기구는 이 개념에 주의를 기울일 것이다. 따라서 이 개념을 숙지하고 그에 따라 정보처리 절차를 개발해야 한다.
6. **투명성 - 정보주체는 자신의 개인정보에 어떤 일이 벌어지고 있는지 항상 알아야 한다.** 광범위한 통지 의무는 GDPR의 적용을 받는 모든 기업에게 매우 어려운 과제가 될 수 있다. 따라서 초반에 이 개념을 숙지할 것을 권장한다.

7. **정보주체의 권리 강화 - 이를 인지하고 대비한다!** 기업은 GDPR에 따른 정보주체의 새롭고 매우 포괄적인 권리를 보장하기 위한 체계를 구축해야 한다.
8. **개인정보 침해 - 특정 요건은 구체적인 보고 절차와 계획을 요구한다.** 예를 들어 GDPR은 개인정보 침해가 발생하는 경우, 컨트롤러(Controller)가 72시간 안에 이를 감독기구에 통지할 것을 규정한다. 신뢰할 수 있는 프로세스를 마련하지 않는 경우, 72시간의 요건을 충족하기 어려울 수 있다. 미리 개인정보 침해에 대한 프로세스를 준비하여 긴급상황에 대비하는 것을 권장한다.
9. **그룹 내 이전 - 동일 회사 그룹 내라고 하더라도 개인정보 이전에 대한 특혜는 없다.** 많은 기업이 믿고 있는 것과는 반대로 같은 회사 그룹 내 기업 간에 개인정보를 이전하는 경우, 제3자에게 개인정보를 이전하는 것과 같은 규칙을 따라야 한다. 개인정보의 이전을 관리하기 위해 개인정보 처리 계약을 체결한다.
10. **국제 개인정보 이전 - GDPR에서 한국은 아직 안전한 제3국이 아니다.** 개인정보를 외국으로 이전하기 전에 GDPR 제44조와 그 이하 조항에 따른 특정 규정을 준수해야 한다. 예를 들어 소위 표준 계약 조항(SCCs)에 기초한 특별 계약을 체결함으로써 준수하여야 한다. 그러나 우리 기업은 상당수 이를 간과하는 경향이 있다.
11. **개인정보 파기 - 지금까지 관행적으로 잘못되어 왔던 개인정보 수집 및 저장은 GDPR 적용 이후 금지된다.** 개인정보가 더 이상 필요 없거나 사용할 수 없는 경우, 해당 정보를 삭제하여야 한다. 적절한 개인정보 보유 및 삭제는 GDPR의 주요 요건이다.
12. **GDPR은 위험 가능성을 고려한 접근법을 요구한다!** GDPR을 준수하기 위해, 일부 보편적인 규정만을 따르는 것은 부족할 수 있다. GDPR은 한 명 또는 그 이상의 개인정보를 보호하기 위해 만들어졌다. 따라서 어떤 조치를 취해야 하는지 판단하기 위해서는 구체적인 상황을 철저히 조사해야 한다. 즉, 실제 처리하고 있는 개인정보의 흐름을 분석하는 것이 중요하다. 이러한 접근법을 따르지 않는 경우, GDPR을 준수하지 못할 가능성이 크다.

III GDPR 전문용어 정리

GDPR의 각 조항에서는 기술적인 용어가 많이 사용되고 있다. 따라서 GDPR 조항을 이해하기 위해서는 먼저 용어를 이해하는 것이 중요하다.

책임성(Accountability) - 개인정보의 (적법한) 처리와 관련한 원칙을 준수했는지 입증할 책임은 컨트롤러에게 있으며, 컨트롤러는 이를 입증할 수 있어야 한다.

정확성(Accuracy) - 개인정보 처리와 관련한 원칙 중 하나로, 개인정보는 언제나 정확해야 하고 필요한 경우 최신의 개인정보를 유지해야 함을 의미한다.

익명처리(Anonymisation) - 정보주체를 식별할 수 있는 개인정보의 파괴. 정보주체를 다시 확인할 수 있는 가명처리와 달리 개인 정보를 익명처리하는 경우, 일반적으로 개인 정보를 더 이상 정보주체에 다시 할당할 수 없거나, 할당할 수 있는 경우에도 엄청난 노력을 해야 한다.

동의(Consent) - 자유롭고 구체적이며, 사전정보에 기반하고 명확한 의사표시가 포함된 정보주체의 의지, 또는 개인정보 처리를 허용하는 정보주체의 적극적이고 긍정적인 행위

개인정보 침해(Data breach) - 보안 위반이나 정보주체의 열람권 침해로 인해 우발적 또는 불법적으로 개인정보를 파괴, 손실, 변경 또는 무단으로 공개하거나 열람하는 것. 이러한 개인정보 침해 발생 시, GDPR 제33조 및 34조에 따라 일정 기간 내에 이를 감독기구와 정보주체에게 보고

개인정보 컨트롤러(Data Controller) - 개인정보 처리의 목적과 수단을 결정하는 주체

개인정보 이동권(Data Portability) - 컨트롤러가 정보주체에게 해당 개인정보의 사본을 제공할 때 다른 컨트롤러가 쉽게 사용할 수 있는 형태로 제공해야 한다는 요건

개인정보 프로세서(Data Processor) - 개인정보 컨트롤러를 대신하여 개인정보를 처리하는 주체

개인정보 처리 계약(Data Processing Agreement, “DPA”) - 개인정보 컨트롤러가 개인정보 프로세서에게 개인정보 처리에 대하여 위탁하기 위해 체결하는 계약. 이 계약은 계약주체, 처리 기간, 처리의 성격과 목적, 개인정보의 종류와 정보주체, 컨트롤러와 프로세서의 의무와 권리, 그 외 사전에 정의한 다른 주제를 포함해야 한다. 일반적으로 표준 계약을 사용한다.

개인정보 영향 평가(Data Protection Impact Assessment, “PIA”) - 개인정보 처리 작업이 미치는 영향을 실제 개인정보 처리 이전에 평가하는 것. 이는 위험 가능성이 높은 상황(예: 정보주체에 대해 상당한 영향을 미치는 새로운 기술이나 프로파일링(profiling) 작업)에서 주로 요구된다.

Data Protection Officer (“DPO”) - GDPR의 준수 여부를 감독하고 이를 수행하는 데 필요한 지식, 자원 및 권한을 가지고 있는 (내부 또는 외부의) 사람

정보주체(Data subject) - 개인정보와 관련이 있는 개인(예: 고용인, 고객 등)

암호화된 개인정보(Encrypted Data) - 특정한 접근 권한이 있는 사람만 접근가능하고 읽을 수 있도록 기술적으로 보호조치가 된 개인정보

GDPR - EU 전역에서 적용되는 EU “일반 개인정보보호법(General Data Protection Regulation)”의 약어

적법성(Lawfulness) - 개인정보를 처리하는데 대한 유효한 법적 근거가 있는 경우(예: 정보주체의 동의, 계약의 체결 또는 컨트롤러의 적법한 이해 추구)에만 개인정보를 처리할 수 있음을 나타내는 원칙

주요 사업장(Main Establishment) - 개인정보의 처리와 관련된 중요한 결정을 내리는 EU내 사업장

개인정보(Personal data) - 간접 식별을 포함하여 식별되거나 식별 가능한 자연인과 관련된 모든 정보

개인정보 보호 적용 설계 및 기본값(Privacy by Design and Default) - 나중에 개인정보 보호를 추가하기보다 시스템 설계 단계부터 개인정보 보호에 대해 고려할 것("적용 설계")을 요구하는 GDPR 개인정보 처리 원칙. 이에 따르면 개인정보를 수집하고 추후에 처리하는 것은 특정한 처리 목표를 달성하기 위하여 필요한 경우로 제한한다(데이터 보호 친화적인 사전 설정)

처리(Processing) - 행위나 작업의 자동화 여부와 상관없이 개인정보에 대해 실시하는 행위나 작업

프로파일링(Profiling) - 개인과 관련된 정보 처리, 또는 개인의 행동(예: 직장에서의 성과, 경제 상황, 건강, 위치 또는 개인적 선호도) 분석 및 예측을 위해 개인정보를 자동으로 처리하는 것

목적 제한의 원칙(Purpose limitation) - 구체적이고 명시적이며 적법한 목적을 위해서만 개인정보를 처리할 수 있는 원칙. 이러한 목적을 위하여 필요한 경우에만 개인정보를 처리("개인정보 처리의 최소화") 및 보관할 수 있다.

가명처리(Pseudonymisation) - 추가 정보(additional data)를 사용하지 않고는 개인을 식별할 수 없도록 개인정보를 처리하는 것. 추가 정보는 별도로 분리 보관되어야 하며 복원(reversible) 키 또는 결합 키(consistent value)를 통해 식별 가능 정보로 되돌릴 수 있는 수단이 된다(예: 해시 값 등).

처리 활동에 대한 기록(Records of processing activities) - 처리 활동에 대한 구체적인 정보(예: 들어 목적, 정보주체, 개인정보, 수령인(recipient) 및 이전)을 포함하는 개인정보 컨트롤러의 기록

정보주체의 권리(Right of the data subject) - GDPR에서 명시하고 있는 정보주체에 대한 권리. 이는 정보를 제공받을 권리, 개인정보를 열람할 수 있는 권리, 개인정보를 정정하고 삭

제할 수 있는 권리, 다이렉트 마케팅(direct marketing)에 반대할 수 있는 권리, 자동화된 의사 결정 및 개인정보의 프로파일링 그리고 개인정보 이동에 반대할 수 있는 권리 등을 포함한다.

제재 규정(Sanctions) - GDPR 위반에 대한 제재 규정으로 물질적 및 비물질적 손해에 대한 법적 책임과 최대 2천만 유로 또는 직전 회계연도 동안 회사 그룹의 전 세계 연간 총 매출액의 최고 4% 중 더 큰 금액의 과징금을 부과한다.

민감정보(Special categories of personal data) - 인종 · 민족, 정치적 견해, 종교적 · 철학적 신념 또는 노동조합 가입 여부를 나타내는 개인정보, 유전자 정보, 생체 정보, 건강 정보, 성생활 · 성적 취향에 관한 개인정보는 원칙적으로 처리할 수 없다. 종종 포괄적 용어인 민감정보를 사용하여 특수한 범주에 속하는 개인 정보와 보호 필요성이 높은 다른 개인 정보를 의미한다. 민감정보는 분실하는 경우, 자연인의 권리와 자유를 위태롭게 할(예: 사기) 가능성이 있는 신용카드와 같은 금융 데이터를 포함한다.

감독 기구(Supervisory authority) - 회원국내 GDPR의 적용을 모니터링 할 책임이 있는 독립된 감독 기구

이전(Transfers) - 유럽 경제 지역(European Economic Area) 역외에 있는 국가로 개인정보를 이전하는 것. GDPR의 조항에 따라 전송하는 경우에만 이전할 수 있다. (예. 한국으로 개인정보를 이전하기 위해서는 표준 개인정보보호조항(Standard Contractual Clauses) 등 추가적 보호조치 후 가능)

IV GDPR 준수를 위한 우리 기업의 조치사항은 무엇인가?

이제 GDPR에 따라 무엇을 해야 하는지를 설명하고자 한다. 유감스럽게도 GDPR을 준수하는 데에 참고할 수 있는 완벽한 계획은 없다. GDPR은 위험 기반 접근법을 채택하기 때문에, 개인정보를 실제로 처리하는 방식과 정보주체의 권리 및 자유에 관한 개인정보 처리 활동의 위험도에 따라 구체적인 요건과 의무는 다르다. 일반적으로 회사의 규모와 산업군이 관련이 있다. GDPR은 사업부문과 회사 규모에 상관없이 적용된다. 따라서 각각의 처리 활동을 검토하고 검토 결과를 평가하며 그 결과에 따라 필요한 조치를 취해야 한다.

하지만 어떤 기업에는 GDPR이 적용되지 않을 수도 있다. 그러나 GDPR이 적용되지 않는 경우(대부분의 경우)에도, 적어도 한국 조직으로써 EU 법률의 적용을 받는 이유와 그 영향이 무엇인지를 알아야 한다.

1 GDPR의 적용 범위는 어디까지인가?

해당 기업이 GDPR의 적용 대상인지 여부를 확인하려는 경우, 다음 두 가지 주요 질문에 대해 검토해야 한다.

- (1) 우리 기업은 개인정보를 취급하는가?
- (2) GDPR의 지리적 적용 범위는 어디까지인가?

1.1 우리 기업은 개인정보를 취급하는가?

GDPR 제2조에 따르면 개인정보 전체나 일부를 자동화된 수단을 사용해서 처리하거나, 자동화된 수단을 사용하지 않더라도 파일링 시스템(filing system)의 일부를 구성하거나 파일링시스템의 일부가 될 개인정보 처리에 대해 GDPR이 적용된다.

즉 GDPR은 거의 모든 개인정보 처리 활동에 적용된다.

1.1.1 개인정보의 처리 - 정의

따라서 개인정보를 사용하는 것이 엄격한 GDPR 규칙의 대상인지를 알기 위해서는 조치가 GDPR에서 규정하는 “개인정보”의 “처리”에 해당하는지를 먼저 결정해야 한다. 이는 말로는 쉽지만 실제로 행하기는 어렵다.

“개인정보”의 “처리”는 다소 광범위하게 해석되어야 하며, 다양한 조치와 여러 범주의 개인정보를 포함한다.

그 자체로는 개인정보가 아닌 정보의 경우(예: 주소나 특정한 장치와 관련한 기술 정보), 해당 정보 간의 조합으로 정보주체를 식별할 수 있는 경우 맥락에 따라서는 개인정보로 간주한다. 예를 들어 IP 주소(인터넷 프로토콜 주소)는 개인정보로 간주한다. 언뜻 보기에는 IP 주소가 자연인에 대한 정보를 드러내지 않더라도 특정 상황에 따라서는 IP 주소를 통해 장치 사용자를 추적할 수 있다(예: 관련기구에서 IP 주소를 요구하는 경우). 이는 ID(SIM 카드나 IMEI 번호와 같은)가 연결된 휴대전화 등의 장치에도 적용된다. 유럽 각 부처들은 특정 상황에 따라 이를 개인정보로 간주할 수 있다.

GDPR은 모든 자연인(정보주체)의 개인정보를 보호할 것을 규정한다. 이는 개별 고객에 대한 개인정보뿐만 아니라 직원에 대한 개인정보, 그리고 공급회사/서비스 제공회사 직원에 대한 개인정보의 포함을 의미하는데, 이는 종종 간과되는 사실이다. GDPR 적용 여부에 있어서는 B2B의 맥락(예: 사업 파트너 직원의 연락처 정보)에서 개인정보를 처리하는지, B2C의 맥락(예: 서비스를 구매한 개인의 연락처 정보)에서 개인정보를 처리하는지는 중요하지 않다는 점을 유의해야 한다.

가장 중요한 규칙: 개인정보인지 확실하지 않을 경우, 개인정보이다!
개인정보를 처리할 때(수집, 파기 또는 개인정보와 관련한 다른 활동)마다 GDPR에서
규정한 개인정보 보호 원칙을 적용한다.

■ 주요 정의 및 예시

“개인정보”

개인의 이름과 연락처 정보는 개인정보의 전형적인 예이다. 개인의 성별, 고객의 구매 이력 또는 사진 등의 정보도 개인정보로 취급한다. 사업 상대의 이메일 주소도 개인정보로 간주할 수 있다. B2B 관계에서만 정보를 처리해야 하며 이에 대한 예외는 없다. 이에 따라 업무 연락처의 이메일 주소가 이름과 같이 개인을 식별할 수 있는 정보를 포함하는 경우, 해당 이메일 주소도 GDPR에서는 개인정보로 간주한다(예: “info@[●]”와 달리 개인에게 할당된 이메일 주소).

“정보주체”

고객뿐만 아니라 사업 상대와 직원도 정보주체로 간주한다는 점을 유념해야 한다.

“처리”

수집, 기록, 조직, 구성, 보유, 각색 또는 변경, 검색, 참조, 사용, 전송을 통한 공개(회사 그룹 내 전송을 통한 공개를 포함), 전파 또는 사용할 수 있도록 하는 것, 정렬 또는 조합, 제한, 삭제 또는 파기와 같이 개인정보에 대하여 실시하는 거의 모든 조치가 처리에 포함된다.

1.1.2 GDPR 적용의 예외 - 익명처리된 정보(Anonymised Data) 및 가명처리 (Pseudonymisation)

개인정보와는 대조적으로 익명처리된 정보를 처리하는 데는 GDPR을 적용하지 않는다.

익명처리된 정보란 무엇이며, 가명처리란 무엇인가?

익명처리된 정보로 간주하기 위해서는 해당 정보를 더 이상 특정 정보주체에 대한 것으로 간주할 수 없어야 한다. 다시 말해 개인을 식별할 수 없거나 개인을 식별하기 위해서는 매우 많은 노력이 필요해야 한다. 이를 위해서는 모든 식별자를 제거해야 하기 때문에, 실제로 정보를 익명처리하는 것은 쉽지 않은 일이다. 특히 정보의 결합/집합과 같이 큰 데이터 셋(빅 데이터)의 경우, 익명처리가 어렵다. 이는 명백하게 개인적이지 않은 정보를 통해서도 정보주체를 식별할 수 있기 때문이다.

개인정보의 익명처리(Anonymisation)에는 무작위화와 일반화와 같은 두 가지 기법을 주로 사용한다.

- 무작위화(Randomisation): 정보와 개인 사이의 강한 연결성을 삭제하거나 모호하게 하기 위해 정보의 정확도를 변경하는 기법

■ 예시

- 정보 값을 상수 기호로 대체한다(예: "*" 나 "x").
- IP 주소 중 일정 수의 비트를 삭제한다(예: IPv4에서 8비트).

- 일반화(Generalisation): 정보주체의 속성을 약화시킨다.

■ 예시

도시 대신에 지역을 수집하거나 구체적인 날짜보다는 달을 수집한다.

익명처리된 정보로 간주되는 경우, GDPR 및 그 엄격한 요건을 그 자체로는 적용하지 않는다.

익명처리된 정보와는 달리, 가명처리된 정보에는 GDPR이 적용된다. 가명처리는 추가적 정보(식별자)를 사용하지 않고는 개인정보와 특정 정보주체를 더 이상 연결할 수 없는 방식으로 개인정보를 처리하는 것을 의미한다.

■ 예시

고객의 이름 및 연락처와 같은 정보를 참조 번호로 대체하고, 단 한 사람이나 해당 집단과 관계없는 사람만 참조 번호를 할당하는 규칙을 알도록 한다.

가명처리된 정보도 여전히 GDPR의 대상이라는 점을 유념한다. 이는 가명처리된 정보의 재식별 위험성이 익명처리된 정보의 재식별 위험성 보다 더 크기 때문이다. 그럼에도 불구하고 가명처리는 개인정보 보호 적용 설계, 개인정보 처리의 최소화 등 GDPR에 따른 의무를 이행하는 방법 중 하나이다. 컨트롤러의 정당한 이익 추구에 따라 개인정보를 처리하는 경우, 가명처리는 특히 도움이 될 수 있다(GDPR 제6조 제(1)항 제(f)호, 세부 사항에 대해서는 다음 참조). 따라서 가능한 경우에는 항상 가명처리를 고려해야 한다.

상기 맥락에서 개인정보를 처리하는 경우, 소위 GDPR의 “주요 적용 범위”에 해당된다.

1.2 GDPR의 지리적 적용 범위는 어떻게 되는가?

위의 첫번째 질문보다 더 긴급한 두 번째 질문은 다음과 같다. 한국 기업도 GDPR의 영향을 받는가? 한국 기업도 GDPR의 지리적 적용 범위 내에 있는가?

GDPR의 지리적 적용 범위는 매우 광범위하며 유럽의 경계를 넘어선다(GDPR 제3조 참조). 원칙적으로 다음의 두 경우에 GDPR이 적용된다.

우선, EU 역내에 기업의 사업장이 있는 경우에는 항상 GDPR이 적용된다(소위 사업장 원칙). 비록 관련 개인정보가 EU 역외에서 처리되더라도 이 원칙을 적용할 수 있다(GDPR 제3조 제(1)항). 사업장에 해당하기 위해서는 인적 자원과 물질 자원을 안정적으로 마련해야 한다. EU 역내에 있는 사업장이 반드시 개인정보 처리에 적극적으로 참여할 필요는 없다(예: 개인정보를 보유하는 것). 하지만 EU 역내에 있는 사업장이 부차적인 서비스(예: 판매 또는 마케팅)를 제공함으로써, EU 역외에 있는 다른 사업장이 관련 개인정보를 처리하는 것을 지원한다면 충분한 요건이 된다. 이는 유럽 개인정보 감독기구가 밝힌 매우 엄격한 견해이다(GDPR (제3조)의 지역적 범위에 대한 2018/3 지침 4페이지 이하와 EDPB를 비교한다. 상세한 사항에 대해서는 아래 제6절을 참조한다). 따라서 안전한 GDPR 준수를 위해서는 다음 해석을 따라야 한다.

반면, EU 역내에 있는 정보주체의 개인정보를 처리하는 경우(비록 역외에서 처리하는 경우에도), GDPR을 적용한다. 지배회사가 EU 역외에 있다는 사실은 이 점에 있어서 관련이 없다. 회사가 EU의 시장과 EU 역내에 있는 고객을 목표로 하는 경우, GDPR의 적용범위에 해당할 가능성이 매우 크다. 예를 들어 EU 역외에 있는 기업이 재화나 서비스를 EU 역내에서 제공하는 경우나 EU 역외에 있는 기업이 EU 역내에 있는 개인의 행동을 모니터링하는 경우(예: 웹 타겟팅 등을 포함하는 온라인 서비스(웹페이지)를 통하여 개인정보를 수집하는 경우), 해당 기업이 GDPR의 적용 범위에 포함될 가능성은 매우 크다.

유럽과 관련된 거의 모든 것이 GDPR의 적용 대상이기 때문에, 기업은 GDPR의 적용 범위에 해당할 가능성이 크다.

■ 비(非) EU 기업의 대리인 임명

GDPR의 지리적 적용범위에 해당하나 EU에서 사업체를 설립하지 않은 경우, GDPR 제 27조에 따라 EU 내 대리인 지정을 고려해야 한다. GDPR 제4조제17항에 따른 “대리인”은 GDPR에 따른 각 의무와 관련하여 컨트롤러나 프로세서를 대표하는 자연인이나 유럽 EU에서 설립한 법인을 의미한다. 이는 감독기구와 정보주체에게 EU 역내 연락 지점을 보장하기 위해서이다.

아래에서 설명하는 바와 같이 컨트롤러와 프로세서에게 의무를 적용한다.

기본 요건은 다음과 같다.

- 대리인을 EU 역내에서 서면으로 지정해야 한다. “대표”하기 위해서는 위임장이 필요하다.
- 이해가 상충하지 않는 한 명의 대리인이 여러 컨트롤러 및/또는 프로세서를 대표할 수 있다고 법률은 규정한다.
- GDPR에 따라 개인정보의 처리를 시작하기 전에 대리인을 지정해야 한다.
- 전문 서비스 제공회사가 대리인 역할을 할 수도 있다. 인터넷 검색이나 KOTRA의 소개를 통해 이러한 전문 서비스 제공회사를 찾을 수 있다.

개인정보를 단지 간헐적으로 처리하는 경우나 건강 정보 또는 침입적 기술(예: 빅 데이터, GDPR 제27조 제(2)항 참조) 등 중요 정보를 포함하지 않는 경우, 예외적으로 대리인을 지정 규정이 적용되지 않을 수도 있다.

1.3 GDPR에서 말하는 개인정보란 무엇인가?

개인정보를 처리하거나 개인정보 처리를 관리하는 모든 자에게 주체의 법적 형태와 상관 없이 GDPR을 적용하기 때문에 그 적용 범위는 매우 넓다. 하지만 GDPR에 따른 역할과 실제 개인정보 보호 책임을 정확하게 알기 위해서는 먼저 GDPR의 맥락에서 귀사가 “컨트롤러”인지 “프로세서”인지를 판단해야 한다.

1.3.1 컨트롤러(Controller) - 컨트롤러가 누구인가?

GDPR 제4조 제7항에 따르면 “컨트롤러”란 자연인, 법인, 공공 기관, 개인정보를 처리하는 목적과 의미를 단독으로 또는 다른 단체나 조직과 공동으로 결정하는 단체나 조직을 의미한다.

따라서 컨트롤러인지 여부는 개인정보 처리 행위 자체가 아니라 의사 결정권을 갖는지에 달려있다. 그러므로 이는 개인정보를 처리하는 목적 및 수단과 관련한 명시적 또는 묵시적 법적 책임이나 실제 영향력에서 비롯될 수 있다. 컨트롤러 여부를 판단하는 또 다른 지표는 타 회사를 위하여 개인정보를 처리하는 것이 아니라 자신의 사업 목적을 위하여 개인정보를 처리하는가 하는 점이다.

■ 예시

인터넷 아울렛을 운영하고 EU 지역의 고객에게 상품을 판매하는 한국 기업이 고객 이름, 주소, 지불 정보 등과 같은 개인정보를 처리하는 수단을 결정하면서(예: 기술적이고 관리적인 측면에서) 자사의 사업 목적을 위하여 이러한 개인정보를 처리하는 경우, 컨트롤러로 간주한다. 이 정보처리가 상품의 판매와 관련이 있는 경우, 이는 자신의 사업 목적을 위한 것으로 본다.

다음 체크리스트를 통해 귀사가 컨트롤러인지 여부를 확인한다.

■ 체크리스트

- ☑ 누가 정보처리의 목적과 그 필수 요소를 결정하는가? 자사가 결정하는가 아니면 다른 기업이 결정하는가? 다른 기업이 결정하는 경우, 해당 기업과 자사와의 관계는 무엇인가?
- ☑ 개인정보의 처리기간을 누가 결정하는가?
- ☑ 누가 개인정보를 열람할 수 있는지, 그리고 어떤 보안 조치를 취해야 하는지에 대한 결정은 누가 하는가?
- ☑ 귀사의 사업 목적과 관련하여 개인정보를 처리하는가, 또는 다른 기업의 사업 목적을 위하여 서비스를 제공하고, 개인정보를 처리하는가?

컨트롤러는 GDPR에 따라 개인정보 보호원칙을 준수할 책임이 있으며, 이 원칙을 준수하고 있음을 입증할 수 있어야 한다.

컨트롤러가 유념해야 하는 가장 중요한 개인정보 처리 원칙은 다음을 포함한다.

■ GDPR 제5조에 명시된 개인정보 처리 원칙

- 적법성
- 공정성 및 투명성
- 개인정보 처리의 최소화
- 처리한 개인정보의 정확성
- (시간적) 보관기간 제한 및 무결성
- 개인정보의 기밀성

특히 컨트롤러는 개인정보를 보호하기 위하여 적절한 기술적이고 관리적인 조치를 취하고 처리의 성격, 범위 및 목적과 자연인의 권리 및 자유에 미칠 위협의 가능성과 심각성을 고려할 책임이 있다(GDPR 제25조 및 제32조 참조).

상기 내용은 개인정보 처리 원칙에 대하여 간략하게 살펴본 것이다. 다음에서 더 상세하게 살펴보고자 한다.

또한 컨트롤러로서 개인정보를 처리할 것을 다른 기관이나 회사에 요청하는 경우, 컨트롤러는 GDPR 제28조에 따른 서면 계약서에 기초하여 프로세서가 특정 개인정보 처리 기본 원칙을 준수하도록 하여야 한다. 이런 계약은 법률이 사전에 규정한 여러 요점을 포함하여야 한다(GDPR 제28조 참조).

1.3.2 공동 컨트롤러(Joint Controller) - 무엇이 다른가?

여러 개인정보 컨트롤러가 개인정보 처리의 목적과 수단을 공동으로 정의하는 경우, “공동 컨트롤러”가 된다. 이는 유럽 법률에서도 상당히 새로운 메커니즘이기 때문에 그 적용 여부에 대해서는 아직 불명확한 점이 있다. 가장 중요한 규칙은, 두 개 이상의 기업이 개인정보 처리 활동을 설계하고 수행하기 위하여 밀접하게 협력하는 경우, 공동 컨트롤러의 직을 고려해야 한다는 점이다. 회사 그룹 내 여러 기업이 중앙 집중화된 절차를 통하여 개인정보를 공동으로 처리하는 경우에도 마찬가지이다. 다시 한번 강조하지만, 개별 사안별로 철저하게 검토할 필요가 있으며, 법적으로 복잡한 사안에 대해서는 전문적인 법적 지원을 받을 것을 권장한다.

이는 매우 중요한 문제이다. GDPR 제28조와 관련하여 위에서 설명한 바(아래 GDPR 제28조에 따른 계약 체크리스트 참고)와 유사하게, GDPR 제26조는 공동 컨트롤러가 구체적인 계약을 체결하여야 하며 그렇지 않은 경우, 관련 당국이 공동 컨트롤러에 이의를 제기하고 벌금을 부과할 수 있음을 규정한다. 이러한 계약은 매우 투명해야 하며, 누가 어떤 개인정보 보호 의무를 이행할지를 결정해야 한다. 특히 누가 정보주체의 권리 행사와 정보 제공 의무에 대해 책임이 있는지를 결정해야 한다.

GDPR에 따르면 계약에 따라 업무를 분담한 것과 상관없이 정보주체는 각 개별(공동) 컨트롤러에게 자신의 권리를 주장할 수 있다. 따라서 공동 컨트롤러가 일부 규칙과 업무에 대해 명확하게 합의할 것을 적극적으로 권고한다.

특정한 계약을 체결하지 않을 경우, 이는 법률을 위반하는 것이며 규제기구는 제재를 가할 수 있다.

1.3.3 프로세서(Processor) - 프로세서란 누구인가?

컨트롤러는 GDPR에 따라 많은 의무를 이행해야 한다. 하지만 프로세서가 되는 기업도 역시 GDPR에 따라 특정 의무를 이행해야 한다.

프로세서는 컨트롤러를 대신해서 개인정보를 처리하며 컨트롤러와는 다른 별도의 법인/개인이다. GDPR 제4조 제7항에 따르면 자연인, 법인, 공공 기관, 단체 또는 조직이 프로세서가 될 수 있다.

컨트롤러는 개인정보를 스스로 처리하거나, 개인정보 처리를 내부 직원이나 부서에 할당하거나, 외부의 제3자(프로세서)에게 위탁할 수 있다. 전형적인 프로세서는 다음과 같다.

■ 예시

- 클라우드 컴퓨팅 공급회사
- 개인정보를 열람할 수 있는 컴퓨팅 센터
- IT 서비스 제공회사
- 반드시 개인정보를 처리하지는 않지만 (이론적으로) 개인정보를 열람하는 소프트웨어 및 IT 서비스의 유지 보수 및 지원 업체

앞에서 설명한 바와 같이 컨트롤러가 프로세서를 고용하는 경우에는 프로세서의 개인정보 전송 및 처리를 포함하는 구체적 계약을 체결해야 한다. GDPR 제28조는 다음 사항을 포함하여 이러한 계약에서 규제해야 하는 요건을 매우 구체적으로 규정한다.

■ GDPR 제28조에 따른 계약 체크리스트

- ☑ 정보처리의 성격, 목적, 대상 및 기간
- ☑ 개인정보의 종류 및 정보주체의 범주
- ☑ 책임자가 지시하는 권한의 범위
- ☑ 기술적 및 관리적 보호조치의 확보
- ☑ 의뢰 받은 정보처리를 완료한 후 개인정보의 반환 또는 삭제
- ☑ 프로세서에 대한 컨트롤러의 통제권
- ☑ 정보주체의 문의 및 요구에 대해, 개인정보 보호 의무의 위반을 의무적으로 보고해야 하는 경우, 계약에 따라 프로세서는 컨트롤러를 지원 할 것
- ☑ (컨트롤러의) 지시가 개인정보 보호법을 위반하는 경우, 이에 대해 프로세서는 정보를 제공할 의무를 가짐

계약서(개인정보 처리 계약)를 작성할 때 위 체크리스트의 내용을 사용할 수 있다. 유럽의 규제기구와 일부 이익 단체는 개인정보 처리 계약 작성 기준으로 참고할 수 있는 표준 계약 템플릿을 발표했다. 하지만 이러한 템플릿을 “있는 그대로” 사용하는 경우 효과가 없을 것이라는 점에 유의해야 한다. GDPR은 위험에 기반한 접근법을 요구한다. 위험에 기반한 접근법이란 개인정보 처리 계약의 내용이 현재 고려하고 있는 사안의 실제 상황을 반영해야 한다는 것을 의미한다.

프로세서가 개인정보를 처리하는 목적을 스스로 결정하는 즉시 프로세서는 스스로 컨트롤러가 되어 컨트롤러의 의무를 이행하여야 하며 컨트롤러로서 의무를 진다. 일반적으로 프로세서는 자사의 목적을 위해 개인정보를 처리할 수 있는 법적 근거가 없으므로, 많은 경우에 문제가 발생할 수 있다. 이러한 목적의 변경이 적법한 경우, 목적의 변경은 GDPR 제6조 제(4)항의 대상이 된다. GDPR 제6조 제(4)항은 당초 수집 목적과 다른 목적으로 개인정보를 처리하는 경우에 대하여 규정한다.

■ 예시

프로세서가 컨트롤러를 대신해서 개인정보를 처리하기 위해 개인정보를 수신한다(GDPR 제28조). 이 때 프로세서가 자사의 사업을 위한 빅 데이터를 분석하는 데 해당 개인정보를 사용할 것을 결정한다면, 컨트롤러를 “대신하여 처리하는 것”의 범위를 벗어남에 따라 후자는 GDPR이 개인정보 프로세서에게 부여하는 권한에 포함되지 않는다. 프로세서는 정보처리에 대한 법적 근거를 제공해야 하며(GDPR 제6조), 해당 정보처리에 대해 정보주체에게 적절하게 통지함으로써 이에 반대할 수 있는 기회를 정보주체에게 주어야 한다(GDPR 제21조 참조). 많은 경우에 프로세서는 요건을 충족할 수 없을 것이다. 따라서, 이러한 종류의 처리 활동은 신중하게 이루어져야 한다.

2 개인정보의 적절한 처리절차

이제까지 GDPR의 맥락에서 귀사가 개인정보를 처리하는지 여부를 판단하는 방법과, 다른 관련된 측면을 고려할 때 GDPR의 적용을 받는지 여부를 판단하는 방법에 대해 알아보았다. GDPR은 다음과 같은 간단하지만 효과적인 원칙을 따른다.

적법한 이유가 없는 경우, 모든 개인정보 처리 활동을 금지한다.

모든 정보처리 활동이 GDPR이나 다른 적용 가능한 법률이 허용하는 바(“법적 근거”)에 해당한다는 점을 입증하는 것은 종종 어려울 수 있으며, 적법한 법적 근거를 정하는 것은 다소 복잡할 수 있다. 하지만 “법적 근거”에 따라 개인정보를 처리하더라도 개인정보의 적법한 처리에 대한 기본 원칙 역시 준수하여야 한다. 또한 개인정보의 처리에 대한 원칙을 준수한다는 것을 GDPR에 따라 입증할 수 있어야 한다. 이를 “책임성”이라고 부른다.

이제 이를 살펴보자.

2.1 일반적인 개인정보 취급 시

개인정보를 처리하기 위해서는 적합한 법적 근거를 결정해야 한다. 개인정보의 처리가 적법하다고 법이 판단하는 특정한 경우나 최소한 이와 유사한 경우에 해당 법률 규정이 법적 근거가 될 수 있다. 이를 확인할 때 고려하는 주요 법적 근거는 GDPR 제6조 제1항에 명시되어 있다.

GDPR 제6조 제(1)항

다음 각 호의 어느 하나에 해당하는 경우, 개인정보의 처리는 적법하다.

- (a) 정보주체가 하나 이상의 특정한 목적을 위하여 자신의 개인정보 처리에 동의한 경우
- (b) 정보주체가 당사자인 계약의 이행을 위해 또는 계약을 체결하기 전에 정보주체의 요청에 따라 조치를 취하기 위해 처리가 필요한 경우
- (c) 컨트롤러에게 적용되는 법적 의무를 준수하기 위해 처리가 필요한 경우
- (d) 정보주체 또는 다른 자연인의 중대한 이익을 보호하기 위해 처리가 필요한 경우
- (e) 공익을 위해 수행되는 직무의 이행을 위해 또는 컨트롤러에게 부여된 공적 권한을 행사하기 위해 처리가 필요한 경우
- (f) 보주체가 아동인 경우처럼 개인정보의 보호가 필요한 정보주체의 이익이나 기본권 또는 자유가 그 이익보다 우선하는 경우는 제외된다.

법적 근거 없는 개인정보 처리는 불법행위로 간주하고, 법적 근거 없이 수집한 개인정보를 사용해서는 안 되며 이는 즉시 파기해야 한다. 과거 법률에 따라 적법하게 수집한 개인정보라 할지라도, GDPR에서 더 이상 허용하지 않는 경우 역시 이를 적용해야 한다.

따라서 특정한 정보처리에 대해 상기 "법적 근거" 중 하나를 활용할 수 있는지를 결정하기 위해서는 다음을 확인할 것을 권고한다.

■ 체크리스트

- ☑ 모든 개인정보의 처리가 법적 근거에 기초하는지를 확인한다.
- ☑ 여러 목적을 위해 개인정보를 수집하고 처리할 수 있다는 것에 유의한다. 적절한 법적 근거를 결정하기 위해서는 특정한 목적과 (해당 목적을 위하여 구체적으로 처리하는) 개인정보에 따라 구별해야 한다. 일반적 접근법은 GDPR에서 효과가 없다. 위험에 기반한 접근법을 기억한다!
- ☑ 따라서 모든 데이터와 모든 처리 활동에 대해 상기 목록을 검토하고 위에서 규정한 이유 중 하나를 용한다. 개인정보를 사용하고자 하는 목적을 쉽게 찾을 수 있는 경우, 법률을 준수하고 있을 가능성이 크다.
- ☑ 개인정보를 사용하고자 하는 목적을 찾을 수 없는 경우, 또는 이에 대하여 확신할 수 없는 경우에는 DPO나 변호사의 자문을 구한다.

상기 모든 법적 근거가 개인정보 처리와 관련이 있을 수 있지만 가장 관련이 많은 경우는 다음과 같다.

- 동의에 기초하여 처리하는 경우(제(a)호)
- 계약을 이행하기 위하여 필요한 경우(제(b)호)
- 적법한 이해에 기초하여 처리하는 경우(제(f)호)

다음은 상기 세 가지 주요 법적 근거를 상세하게 설명한다.

2.1.1 언제 계약의 이행에 근거하여 개인정보를 처리할 수 있는가?

개인정보를 수집하고 처리하는 가장 중요한 근거는 일반적으로 (기존의) 계약상 의무를 이행하기 위하여 개인정보를 처리하는 것이다.

많은 경우에 계약을 이행하기 위해서는 개인정보를 처리하게 된다. 이런 정보처리 활동을 제한하는 경우, 일상적인 생활과 사업을 영위하기가 불가능하다. 이에 따라 GDPR은 계약 이행과 관련하여 개인정보를 처리하는 것에 대한 일반적인 법적 근거를 규정한다.

■ 대표적인 예시

구매 계약(예: 서비스의 전달이나 제공)과 관련하여 고객의 이름과 주소를 처리하는 것. 하지만 고객의 성별이나 신발 치수를 처리하는 것은 제외한다(일반적으로 계약을 이행하기 위해 필요하지 않기 때문에).

고객에게 청구서를 보내기 위해 요금 청구 정보를 처리하는 것. 하지만 마케팅 목적으로 요금 청구 정보를 이용하는 경우, 이는 일반적으로 계약을 이행하기 위해 필요하지 않기 때문에 다른 법적 근거가 필요하다.

위에서 살펴본 바와 같이, GDPR은 법률을 다소 엄격하게 해석한다. 계약의 이행에 근거하여 개인정보를 처리하기 위해서는, 개인정보 처리가 계약상 목적을 달성하기 위해 반드시 필요해야 한다. 다른 목적을 위해 처리하는 경우에는, 더 이상 계약상 의무를 이행하기 위한 정보처리에 해당하지 않는다.

둘째, 개인정보를 처리하는 정도를 다른 개인정보 처리 원칙("목적 제한의 원칙" 및 "개인정보 처리의 최소화")과 같이 계약을 이행하기 위하여 필요한 정도로 제한한다.

■ 예시

상품이나 서비스를 온라인으로 판매하고 고객이 온라인 쇼핑물에 등록해야 하는 경우, 개인정보의 수집범위는 거래를 이행하기 위해 필요한 정도로 제한해야 한다. 생년월일을 요구하는 것은 온라인 쇼핑물에는 유용할 수 있으나, 일반적으로 생년월일 정보가 정말 필요한 경우는 없다. 고객의 생일에 이메일을 보내기 위해 생년월일 정보를 수집하고자 하는 경우, 이는 다른 "목적" (일반적으로 마케팅과 관련하여)을 위한 것이기 때문에 "계약" 이외의 다른 법적 근거가 있어야 한다는 것에 유의해야 한다.

마지막으로, 계약(및 계약 이후 의무)의 이행을 완료한 후에는 개인정보를 계속 보유할 수 있는 법적 근거가 없다. 따라서 GDPR에 따라 다른 목적을 제시할 수 없는 경우, 개인정보를 삭제해야 한다(보유 기간 제한의 원칙). 이는 일반적으로 매우 제한적인 상황이다(GDPR 제6조 제(2)항 참조). 이는 개인정보를 수집할 때 개인정보를 수집한 목적이 중단 되는 경우(예: 계약을 이행한 경우)에 개인정보를 삭제하기 위한 계획을 이미 수립해야 함을 의미한다.

요약하면, 법적 근거로써 “계약”을 평가할 때, 다음 사항을 확인해야 한다.

■ 체크리스트

- ☑ 정보주체와 계약관계(예: 구매 계약이나 서비스 계약)가 있는지를 확인한다. 계약관계가 없는 경우, 일반적으로 GDPR 제6조 제(1)항 제(b)호를 적용하지 않는다.
- ☑ 계약상 목표를 달성하기 위해 필요한 개인정보만 수집하며, 꼭 필요한 개인정보만 수집하도록 제한한다.
- ☑ 세부 사항이 중요하다. 개인정보를 철저히 분석하고 항상 전체적인 맥락을 평가한다. GDPR은 위험에 기반한 접근법을 사용한다. 따라서 귀사가 하는 일에 대해 정확히 파악하지 못하는 경우에는 GDPR을 준수할 수 없음을 명심해야 한다.

2.1.2 왜 동의가(Consent) 필요하며 동의는 어떻게 작동하는가?

정보주체와 계약관계가 없는 경우, 동의는 개인정보를 적법하게 처리할 수 있는 법적 근거 중 하나가 될 수 있다. 개인정보 처리 활동은 동의를 통해 언제나 합법화할 수 있지만 동의를 활용하는 데 있어서는 주의가 필요하다. 이는 동의를 받는 것이 상업적으로 불가능할 수 있을 뿐만 아니라 법적 위험을 부담해야 할 수도 있기 때문이다. 따라서 다른 법적 근거를 통하여 처리 활동을 합법화할 수 있는 경우, 컨트롤러 또는 제3자의 적법한 이익 추구를 위한 경우(아래 참조)와 같은 다른 법적 근거를 통해 처리 활동을 합법화해야 한다.

다른 법적 근거를 활용할 수 없는 경우에만 동의를 활용한다.

이는 유효한 동의를 받는 데 대해 GDPR이 엄격한 요건을 규정하고 있으며, 이러한 동의는 언제든지 철회할 수 있다는 사실 때문이다. 아래에서는 동의에 대하여 단계별로 설명하고 있다.

첫째, 유효한 동의는 GDPR 제7조에서 규정한 기준을 충족해야 한다.

■ 동의를 기본 요건은 무엇인가?

- **동의를 자유롭게 제공되어야 한다.** 동의를 제공하는 데 있어서 정보주체는 선택권을 가져야 한다. 일반적으로 **동의에 다른 조건을 추가해서는 안 된다.** 예를 들어, 동의를 제공하는 조건으로 서비스 유료 제공을 추가해서는 안 된다. 예외가 있을 수 있지만, 매우 드물게 인정된다!
- **하나의 구체적인 목적에 대해서만 동의를 받을 수 있다.** 하나의 동의에 여러 목적을 포함시키기 위해서는 정보주체가 모든 목적이나 그 일부를 선택할 수 있어야 한다.
- 동의를 **명료**해야 한다. 의미가 명료하고 쉽게 열람할 수 있는 서식에서 명료하고 이해하기 쉬운 언어를 사용하여 다른 사안과 분명하게 구별할 수 있는 방식으로 동의를 받아야 한다.
- **분명**해야 한다 - 처리의 목적, 사용할 개인 정보 및 처리에 참여하는 주체를 표시한다.
- 동의하기 전에 정보주체는 동의를 철회할 수 있는 권리와 그 결과에 대한 정보를 제공 받아야 한다.

동의를 자유롭게 제공하는지에 대한 판단은 개별 사례에 따라 다르다. 정보주체가 불이익을 받을 가능성이 있는 경우, 동의를 자유롭게 제공한다고 추정할 수 없다. 고용 관계에 있어 이는 특히 중요하다. 이는 임직원의 경우, 대개 자신의 직책을 보호하기 위해 동의하기 때문이다. 따라서, 이러한 경우의 동의는 자유롭게 제공하지 않은 것으로 간주한다.

■ 예시

임직원의 사진을 고객에게 보여주기 위해 회사 웹사이트에 게재하고자 한다. 이를 위해서는 일반적으로 동의가 필요하다.

동의를 받는 절차를 어떻게 설계하는지에 따라 임직원에게 선택권이 없어서 유효한 동의로 간주되지 않을 수도 있다.

이 문제에 대한 해결책은 임직원에게 불이익 없이 동의할(또는 동의하지 않을) 수 있는 선택권을 제공하는 것이다. 이런 경우, 선택의 자유가 있는 것이다! 불이익이 없음을 보장해야 한다. 어떤 경우에도 처리에 관한 모든 정보(사진을 누구를 위하여 어디에 게재할 것이며 얼마나 오랫동안 게재할 것인지)를 사전에 임직원에게 제공해야 한다.

각 목적에 대하여 동의를 별도로 받아야 한다는 점에 유의해야 한다. 예를 들어 동의에 기초하여 여러 목적을 위해 개인정보를 처리하고자 하는 경우, 여러 개의 체크박스가 있는 서식을 제공해야 한다(하나로 묶을 수 없다).

■ 예시

고객에게 마케팅 이메일을 송부하고 다른 이유 때문에 고객의 개인정보를 파트너 업체와 공유하고자 한다. 이를 위하여 정보주체의 동의를 받고자 하는 경우에는, 예를 들어 동의서에 두 개의 다른 체크박스를 포함시켜야 한다.

책임성에 대하여 설명한 바와 같이, 적합한 방법으로 동의를 받은 것에 대한 사실을 문서화해야 한다. 전자적 수단을 통해 동의를 받는 경우, 이 방법에 대하여 설명할 수 있도록 준비해서 법률을 준수했음을 입증할 수 있어야 한다. 이를 입증할 수 없는 경우, 감독기구(또는 관할 법원)는 귀사가 법률을 위반한 것으로 간주할 수 있다. 따라서 동의를 받는 방법뿐만 아니라 이를 추후에 입증하는 방법을 항상 생각해야 한다.

마지막으로 **동의를 언제든지 철회할 수 있다는 것**을 인식해야 한다. 동의를 철회하는 경우, 동의에 근거하여 처리된 개인정보는 안전하게 파기되거나 익명으로 처리되어야 한다. (적어도 동의에 기초한 경우) 동의를 철회한 이후에는 추가로 처리할 수 없다! 정보주체가 동의를 철회하는 데는 (거의) 제한이 없다는 것을 인식해야 한다.

유효한 동의를 제공하는 데 일부 **연령 제한**이 있을 수 있다는 것에 유의해야 한다. 예를 들어 상품이나 서비스를 아동에게 판매하는 경우, 유효한 동의를 구하는 것이 문제가 될 수 있다. 따라서 상품이나 서비스를 아동에게 판매하는 경우, 항상 전문적인 조언을 구해야 한다. 이는 다소 복잡한 법률적 문제이기 때문이다.

위의 요건을 준수하지 않는 경우, 동의를 유효하지 않은 것으로 여겨지며, 그 결과 개인정보를 불법적으로 처리한 것으로 간주될 수 있다.

요약하면 법적 근거로서 동의를 검토할 경우, 다음 사항을 확인해야 한다.

■ 체크리스트

- ☑ 동의를 받아야 하는지를 항상 철저히 검토한다. 동의를 받는 것은 실효성이 낮은 해결책이다. 다른 옵션을 먼저 고려한다(상기 내용 참조)!
- ☑ 동의를 구할 때는 명료하고 분명한 언어를 사용한다. 사용한 언어는 정확하고 명확해야 한다. 그렇지 않은 경우, 동의를 무효가 될 위험이 크며 이에 따라 개인정보 처리도 무효가 될 수 있다!
- ☑ 2018년 5월 이전에 이미 동의를 받은 경우, 동의를 필요하지 그리고 적법하게 동의를 받았는지를 확인한다. “과거”에 받은 동의를 GDPR의 요건을 준수하지 않은 경우, 이는 무효이다. 과거에 받은 동의를 GDPR의 요건을 준수하는지를 확인할 수 없는 경우, DPO나 외부 변호사의 자문을 구한다.
- ☑ 마지막으로, 위에서 설명한 것처럼 동의를 철회하거나 동의를 무효인 경우에 대한 프로세스(즉 해당 개인정보를 파기하는 절차)를 수립해야 한다.

2.1.3 개인정보를 처리하는 적법한 이익(Legitimate Interest)은 어떤 경우에 있는가?

GDPR은 컨트롤러나 제3자의 적법한 이익에 근거하여 개인정보를 처리하는 것을 허용한다. 이는 법률의 특정한 규칙에 해당하지 않는 개별적인 이익이 있을 수 있다는 것을 법률이 인정한다는 것을 의미한다.

■ 예시

사업 파트너의 지불 능력을 확인하는 것은 적법한 이익이 될 수 있다. 이는 당사자가 합리적으로 예상할 수 있는 것이기 때문이다.

각각의 이익이 적법하고 정보주체의 이익보다 우선할 수 있는지는 개별 사례별로 다르다. 이를 사례별로 결정해야(그리고 문서화해야) 한다.

정보주체의 나이, 개인정보에 대한 예측과 추론, 민감정보의 존재는 적법한 이익 여부를 고려하기 위하여 필요한 균형 시험을 실시하기 위한 지표 역할을 할 수 있다. 다음과 같은 대표적인 지표는 평가하는 데 도움이 될 수 있다.

- 민감정보(예: 신체적 또는 정신적 건강에 대한 정보)를 처리하는 경우, 정보주체의 이익이 다른 이익보다 우선할 가능성이 더 크다.
- 개인정보를 이미 온라인에서 열람할 수 있는 경우, 사소한 이익도 당사자의 이익보다 우선할 수 있다.
- 가장 중요한 지표 중 하나는 개인정보 처리에 대한 정보주체의 예측 범위이다. 예를 들어 EU 내 사용자는 자신이 웹사이트를 사용하는 행동이 분석의 대상이 될 수 있다는 것을 예측할 수 있지만 자신이 웹사이트를 사용하는 행동에 대해 프로파일이 생성되며 그 프로파일이 제3자에게 판매된다는 것을 예측하지는 못할 수도 있다.

가장 중요한 규칙은 정보주체의 프라이버시에 대한 영향이 크면, 컨트롤러 또는 제3자의 이익도 그에 상응할 만큼 중요해야 한다는 것이다.

예를 들어 전적으로 경제적 이익은 안정적이고 안전한 서비스를 제공하는 이익보다 덜 중요할 수 있다.

GDPR은 일부 적법한 이익을 정의한다. 이런 이익은 일상적인 경영 활동(직접적인 마케팅 활동 실시 또는 관리 목적으로 회사 그룹 내에서 개인정보를 이전하는 적법한 이익을 포함하는)에서 매우 중요하다. 이런 조항을 다소 엄격하게 해석해야 한다는 점을 유념할 필요가 있다.

법적 근거를 선택할 수 있는 경우, 계약 이행이라는 법적 근거에 기초하여 처리하는 것을 권장한다. 정보주체는 적법한 이익에 기초한 정보처리에 대해 반대할 권리가 있다(GDPR 제21조).

■ 체크리스트

- ☑ 법적 근거로서 “적법한 이익”을 고려하는 경우, 다른 법적 근거(특히 계약 이행)에 기초하여 개인정보를 처리할 수 있는지를 확인한다.
- ☑ 적법한 이해에 기초하여 처리하는 경우, 귀사와 정보주체의 이익을 적절하게 고려한다. 민감한 정보일수록 개인정보를 처리하지 않는 것으로 인한 정보주체의 이익이 귀사의 이익에 우선할 가능성이 더 크다.
- ☑ 이러한 고려 사항을 문서화(예: 처리 활동에 대한 귀사의 기록)한다. 이는 감독기구가 문서를 요구할 수 있기 때문이다. GDPR을 준수한다는 것을 입증할 수 있어야 하며 이는 적절한 문서화를 포함한다는 것을 유념한다.

2.2 개인정보 중에서 민감정보(Special Categories of Personal Data) 취급 시

위에서는 개인정보를 처리하는 데 대하여 법적 근거가 있는지를 결정하는 방법을 설명하였다. 아래에서는 일부 범주에 속하는 개인정보에 대해서는 추가적인 보호조치를 취하여야 하며 달리 취급해야 한다는 것을 설명한다.

GDPR은 모든 개인정보를 보호하지만 일부 개인정보는 특별한 방식으로 보호한다. GDPR 제9조에 따르면, 민감정보에는 자연인을 고유하게 식별하기 위한 인종 또는 민족, 정치적 의견, 종교적 또는 철학적 믿음, 노동조합 가입 여부, 유전 또는 생체 정보를 보여주는 개인정보, 건강에 대한 개인정보, 자연인의 성생활이나 성적 지향에 대한 개인정보 등이 있다. GDPR 제9조는 더 엄격한 요건을 규정하며 이런 민감정보를 처리하는 것을 근본적으로 금지한다(GDPR 제9조 제(1)항). GDPR 제9조 제(2)항에 따르면 예외는 매우 제한적인 경우에만 허용된다. 이런 종류의 개인정보는 특히 중요하기 때문에 각별한 보호를 받을 가치가 있다. 이러한 개인정보를 주의하여 처리하거나 남용을 방지하지 않는 경우, 정보주체의 기본권과 자유를 침해할 위험이 상당하다. 이는 기구, 고용주, 보험회사 또는 다른 기관이 정보주체의 종교, 정치적 견해 또는 건강 상태에 따라 정보주체를 차별하지 않도록 보장하는 것이다.

가장 중요한 규칙은 특정한 사업 분야에서 처리하는 것을 제외한 경우(예: 치료를 위하여 반드시 필요한 경우 또는 고용 관계에서 개인정보를 처리하는 것을 허락하여야 하는 경우), 정보주체의 명시적 동의에 따라 민감정보를 처리해야 한다는 것이다. 일반적으로, 민감정보는 GDPR 제6조 제(1)항 제(4)호에서 규정한 바에 따라 적법한 이익에 기초하여 처리할 수 없다. 매우 중요한 개인정보의 처리 활동과 피해(GDPR을 준수하지 않는 방식으로 중요정보를 사용하는 경우, 발생할 수 있는)를 GDPR 제9조에서 명시한 규칙에 따라 철저하게 확인할 것을 적극적으로 권고한다.

GDPR 제28조에서 규정한 프로세서로서 행동하는 것과 컨트롤러를 대신하여 민감정보를 처리하는 것을 그 자체로 금지하지는 않는다. 하지만 개인정보 보호기구는 이런 종류의 사업 모델을 매우 엄격하게 평가하고 일정 수준의 기술적 및 관리적 보호조치(예: 개별 계약에 대한 요건과 관련하여)를 취하도록 요구하는 경향이 있다.

요약하면, 민감정보를 다룰 때에는 매우 신중해야 하며 법적 상황을 철저히 평가해야 한다. 다음 체크리스트는 출발점이 될 수 있지만, 이에 대해 항상 DPO 및 변호사와 논의해야 한다.

■ 체크리스트

- ☑ 민감정보를 처리하는 경우, GDPR이 규정하는 구체적인 요건에 주의한다.
- ☑ 이러한 종류의 개인정보를 반드시 수집해야 하는지를 항상 철저히 숙고한다. 이러한 개인정보를 수집할 필요가 없다면, GDPR을 준수하기에 훨씬 수월할 것이다.
- ☑ 민감한 정보를 처리해야 하는 경우, 비록 GDPR이나 법적 구속력이 있는 국가의 법률에 따라 하나의 추가 규칙을 적용할 수 있다는 것을 발견하더라도 GDPR 제9조 제(2)항에서 규정한 법적 요건을 검토하고 고려한다.
- ☑ 민감정보의 처리를 포함하는 일부 처리 활동을 제3자에게 위탁하는 경우, 이를 위해 충족해야 하는 요건을 철저히 평가한다. 예를 들어 병원에 IT 서비스를 제공하고 환자의 개인정보를 열람할 수 있는 경우, 법률은 매우 제한적인 상황에서만 이를 허용한다. 전문가와 함께 개인정보의 보호 관련 법률과 환자의 개인정보 처리에 관한 다른 법률을 상세하게 검토해야 한다.
- ☑ 이런 종류의 개인정보를 불법적으로 열람하는 경우, 일부 국가에서는 형법에 따라 처벌을 받을 수도 있다는 점을 유의한다. 다른 요건도 초기에 철저히 검토해야 한다!

3 개인정보 취급 시 유의해야 할 기본 수칙

위에서는 개인정보를 처리할 때 귀사의 “역할”과 개인정보를 처리하기 위한 적절한 “법적 근거”에 대하여 설명하였다. 하지만 아래에서 설명하는 바와 같이 이것만으로는 충분하지 않다.

이와 더불어 개인정보의 적법한 처리에 대한 기본 원칙도 항상 준수해야 한다. 이러한 기본 원칙을 간략하게 설명하면 다음과 같다.

- 공정성 및 투명성의 원칙
- 목적 제한의 원칙
- 개인정보 처리의 최소화
- 정확성의 원칙
- 보유 기간 제한의 원칙
- 무결성과 기밀성의 원칙

어떤 상황에서도 이러한 개인정보 처리 원칙을 동시에 적용한다. 따라서 GDPR에 따라 개인정보를 처리하기 전에 이런 개인정보 처리 원칙을 숙지해야 한다.

그리고 이러한 개인정보 처리 원칙 중 하나라도 준수하지 않는 경우, 감독기구 등이 과징금과 같은 제재를 부과할 수 있음을 알아야 한다. 일반적으로 GDPR에는 사소한 위반이라는 것은 없다. 따라서 감독기구 등은 모든 종류의 위반에 대해 제재를 부과해야 한다. 개인정보의 처리에 대한 다음과 같은 원칙은 “권장 사항”이 아니라 조치를 취하여야 하는 필수 요건이다.

3.1 개인정보 처리 절차에 대한 투명성 보장

GDPR에 따르면, 정보주체의 개인정보 처리는 투명해야 한다. 처리 활동의 모든 관련 측면에 대한 정보는 정보주체에 제공되어야 한다. 즉, 정보주체의 개인정보를 보유하고 있는지와, 이 개인정보 처리의 용도와 이유에 대한 정보를 정보주체에게 제공해야 한다. 비록 개인정보를 정보주체로부터 직접 받은 것이 아니라 제3자(예: 공개적으로 사용할 수 있는 웹사이트)를 통해 받았더라도 이런 개인정보 처리 원칙이 적용되며, 정보주체에게 이를 통지해야 할 수 있다.

일반적으로 정보주체의 개인정보를 수집하는 경우, 정보주체에게 다음 정보를 제공해야 한다. GDPR 제13조는 다음에 대한 체크리스트의 역할을 할 수 있다.

- 컨트롤러의 신원(일반적으로 기업의 상호, 주소, 연락처 및 대리인)
- 컨트롤러의 DPO에 대한 연락처 세부사항
- 처리 목적과 법적 근거(요약하면 개인정보를 보유하는 이유와 개인정보를 사용하여 하고자 하는 바)
- GDPR 제6조 제(1)항 제(f)호에 의거한 적법한 이익
- 전송 중 개인정보의 수령인(예: 서비스 제공업체)
- 한국 등 제3국(예: 제3국에 있는 모회사)으로의 이전
- GDPR 제13조제(2)항에 따르면 컨트롤러는 다음 정보도 제공하여야 한다.
- 보유 기간(예: 얼마나 오랫동안 개인정보를 유지하고자 하는지 그리고 그 이유)
- 정보주체의 권리(예: 처리에 대하여 반대할 수 있는 권리)
- 동의 철회 가능성(동의를 기반한 경우)
- 감독기구에 이의를 제기할 수 있는 권리(GDPR 제77조)
- 예를 들어 계약을 체결하기 위하여 개인정보를 제공하여야 하는 의무
- 자동화된 의사결정과 프로파일링

불투명한 정보처리 활동은 무효로 판단될 수 있으며 이에 따라 금지될 수 있다. 감독기구 등이 엄격하게 판단하는 경우, 정보처리 전체가 불법이 될 수 있다. 따라서 부정적인 결과를 피하기 위해서는 투명성을 확인할 것을 권고한다.

이미 설명한 바와 같이 조사 시점(개인정보를 구하는 시점)에 정보주체에게 미리 정보를 제공해야 한다. 대부분의 경우, 정보주체의 개인정보를 어떻게 사용할지를 설명하는 “개인정보 처리방침”을 통해 미리 정보를 제공한다. 개인정보 처리방침을 서면이나(예: 한 장의 종이) 전자적 수단을(예: 웹사이트에서) 통하여 제공할 수 있다. 이론상으로는 필요한 정보를 구두로 제공할 수도 있다. 하지만 일반적으로는 구두로 제공하는 것은 권장하지 않는다. 이는 구두로 제공하는 경우, 대개 관련 문서가 없어서 귀사가 GDPR을 준수하는 것을 입증하기가 어렵기 때문이다. 귀사가 콜 센터를 운영하고 법률에 따라 정보주체에게 미리 정보를 제공하는 절차(예: 컴퓨터에 기반하여 정보를 자동으로 읽어주거나 인터넷에 있는 추가 문서를 참조하는)에 정보를 포함시킬 것을 결정하는 경우에는 정보를 구두로 제공할 수도 있다. 이러한 종류의 처리를 고려하는 경우, 상세하게 검토하고 적절한 법적 조언을 구해야 한다. 이는 유럽에서 이러한 요건에 대해 활발하게 논의하고 있기 때문이다.

일반적으로 개인정보 처리방침을 통하여 이런 요건을 준수하기 때문에 이러한 통지 의무는 온라인 절차(현재 개인정보 처리방침을 더 일반적으로 사용하는)에만 적용되는 것이 아니라 오프라인 절차에도 적용된다. 개인정보 처리방침은 정보를 특정한 포맷으로 제공할 필요는 없지만 위에서 설명한 바를 알기 쉽게 설명하여야 한다. 따라서 가장 이해하기 쉬운 방식으로 정보를 제공하는 한 서비스 계약에 첨부된 정보 서식을 이용하여 고객에게 정보를 제공할 수도 있다.

개인정보를 정보주체로부터 직접 구한 것이 아니라 제3자(예: 다른 컨트롤러나 공개적으로 사용할 수 있는 웹사이트)로부터 받은 경우, 추가적인 정보 제공 의무를 적용한다. 컨트롤러는 개인정보를 어떻게 구했는지를 정보주체에게 통지해야 한다(세부사항에 대해서는 GDPR 제14조 참조). 정보주체로부터 직접 개인정보를 받은 경우에 적용하는 규칙은

제3자로부터 개인정보를 구한 경우에 적용하는 규칙과는 다르다(GDPR 제13조 참조). 귀사가 이에 해당하는 경우, 어떤 규칙을 준수해야 하는지를 철저하게 평가해야 한다.

그렇다면 투명성 원칙과 관련해 유념해야 할 사항은 무엇인가? 다음 체크리스트는 이에 대한 개요와 지침을 제공하고 있다.

■ 체크리스트

- ☑ 귀사에게 통지 의무가 있는지를 확인한다. 거의 모든 경우에 통지 의무가 있을 것이다. 예외 사항은 매우 제한적으로 해석된다.
- ☑ 개인정보 처리방침과 통지에 대한 정책을 수립하고 각각의 “정보주체”에 이를 제공하는 절차를 결정한다.
- ☑ 모든 관련 정보를 정보주체에게 통지하고 GDPR 제13조와 제14조를 토대로 필요한 모든 정보를 포함하는 서식을 작성한다.
- ☑ 항상 보다 많은 정보를 제공할 것을 권고한다.
- ☑ 고객, 임직원 또는 사업 파트너는 법률 전문가가 아니라고 간주한다. 분명하고 명료하며 간결한 언어를 사용한다.

3.2 개인정보에 대한 활용 목적의 제한 및 관련 처리 절차의 최소화

구체적인 목적을 위해서만 개인정보를 처리할 수 있으며, 해당 목적을 위해 개인정보를 처리하려면 법적 근거가 있어야 한다.

개인정보를 처음 수집했을 때의 목적이 아닌 다른 목적을 위해 개인정보를 처리하는 경우(예: 계약 이행을 위해 개인정보를 받은 후 이를 마케팅 활동을 위해 사용하는 경우), 별도의 법적 근거를 통하여 각 목적의 적법성을 입증해야 한다. 그 결과 목적을 변경하는 것은 다음의 경우에만 법적으로 허용된다.

- 정보주체의 동의에 기초하는 경우(아래 IV.4 참조).
- 새로운 목적이 최초의 목적과 양립할 수 있는 경우.

■ 예시

고객에게 통지하는 데 사용하기 위하여 고객의 이메일 주소를 수집한다. 또한 마케팅(예: 뉴스레터의 발송)을 위하여 이메일 주소를 사용하고자 한다.

첫 번째 목적(특정 목적을 위한 정보 제공)이 계약 이행을 그 법적 근거로 할 수 있는 반면에 두 번째 목적(뉴스레터의 발송)은 계약 이행을 그 법적 근거로 할 수 없다. 이는 두 번째 목적이 계약 이행과 관련이 없기 때문이다. 따라서 별도의 법적 근거(동의 등)가 필요하다.

또한 개인정보 처리의 최소화 원칙을 모든 정보처리 활동에 적용한다. 이는 특정한 목적을 위해 필요한 개인정보만 처리해야 함을 의미한다. 온라인 서식을 통해 개인정보를 수집하는 경우에는 이 원칙을 잊는 경우가 많다. 예를 들어 간단한 연락처 서식의 경우, 일반적으로 나이나 성별을 물을 필요가 없다. 따라서 이러한 개인정보의 수집은 불법으로 간주할 수 있고, 따라서 이런 개인정보는 파기해야 한다. 또한 개인정보 파기에 대한 개념(시스템에서 개인정보를 파기하는 것을 설명하는 개념)을 설계하기 시작한 경우, 개인정보 처리의 최소화 원칙을 준수하지 않고 수집한 개인정보는 문제가 될 수 있다. 따라서 우선 수집하는 개인정보의 양을 제한할 것을 권고한다.

■ 체크리스트

- 목적을 달성하기 위해 어떤 개인정보가 필요한지를 확인한다.
- 단지 수집 가능하다는 이유로 개인정보를 수집하는 경우, 문제가 될 수 있다.
- 이에 따라 행동할 것을 임직원에게 교육한다.

3.3 개인정보의 정확성 보장

개인정보는 정확해야 하며 필요한 경우 최신 정보여야 한다. 정확하지 않은 개인정보의 경우, 처리 목적을 고려하여 즉시 파기하거나 정정하기 위한 모든 합리적 조치를 취해야 한다.

■ 체크리스트

- 개인정보가 정말 필요한지를 확인하고, 오래되고 부정확한 개인정보를 즉시 삭제하여 중복을 제한하고 개인정보 품질을 적절하게 유지한다.
- 정보주체가 새로운 이름이나 주소 등의 이유로 자신의 개인정보를 정정하거나 열람하고자 하는 경우, 이에 즉시 대응하고 이에 따라 사업절차를 수정한다.
- 높은 서비스 품질을 보장하기 위해 정책을 충분히 수립하고 이를 임직원에게 교육한다.

3.4 개인정보의 보유 기간 제한

개인정보를 처음 수집했던 목적을 달성해 더 이상 개인정보가 필요하지 않은 경우, 안전하게 삭제 또는 파기하거나 완전하게 익명으로 처리해야 한다.

이를 위하여 다음 사항을 이행해야 한다.

- 개인정보를 유지해야 하는 기간과 목적을 평가한다.
- 구체적인 목적을 위해 더 이상 필요하지 않은 정보는 안전하게 삭제한다.

개인정보를 보유하는 적절한 기간을 결정하는 경우, 각 국가의 법률과 구체적인 최소 또는 최대 보유 기간이 최초의 지표 역할을 할 수 있다. 예를 들어 임직원의 세금 기록이나 건강 기록, 분쟁이나 소송과 관련한 문서에 대한 보유 기간은 최초의 지표 역할을 할 수 있다.

책임성의 원칙을 준수하기 위해서는 보유 정책 내에서 개인정보 보유 계획을 문서화하고, 이를 정기적으로 확인 및 업데이트해야 한다. 이를 위해 다음 조치를 취해야 한다.

■ 체크리스트

- ☑ 개인정보를 어디에 보유하고 있는지 확인한다.
- ☑ 얼마나 오랫동안 개인정보를 필요로 하는지(보유 기간)를 결정한다. 개인정보의 범주와 개인정보를 수집한 최초의 목적에 따라 보유 기간은 다를 수 있다. 보유 기간을 결정하는 것에 관한 한 지역의 법률이 오리엔테이션의 역할을 할 수 있다(예: 법률이 규정하는 기록 보관의 경우).
- ☑ 특정 목적을 위하여 더 이상 필요하지 않은 개인정보를 적절한 때에 안전한 방식으로 파기하거나, 가능한 경우, 이런 개인정보를 자동으로 파기하는 절차를 수립한다.
- ☑ 위의 사항을 문서화하는 개인정보 보유 정책을 수립한다.

3.5 개인정보의 무결성 및 기밀성 보장

무단 열람, 손실, 도난 또는 손상으로부터 개인정보를 보호하기 위해서는 적절한 기술적 및 관리적 보안 조치를 취해야 한다. 또한 이러한 목표를 달성할 수 있도록 IT 시스템을 설계해야 한다.

해당 시점에서의 기술 수준, 처리와 관련한 비용, 성격, 범위와 목적 그리고 자연인의 권리와 자유가 변할 가능성과 그 정도를 고려해야 한다. 보호조치는 위험에 상응하는 보안 정도를 보장해야 한다. 이는 법률이 “모든 상황에 보편적으로 적용할 수 있는” 접근법을 허용하지 않으며 오히려 적절한 IT 보안을 보장하기 위해 회사가 개별 절차와 보호조치를 설계할 것을 요구한다는 점을 의미한다.

자세한 사항에 대해서는 아래의 제6절을 참조한다.

3.6 개인정보 보호 적용 설계(Privacy by Design) 및 보호 기본 설정(Privacy by Default)

GDPR은 기존의 보안 요건을 한 단계 더 발전시키고 “개인정보 보호 적용(Privacy by Design)” 원칙 및 “개인정보 보호 기본 설정(Privacy by Default)” 원칙과 같은 예방 메커니즘을 포함한다.

개인정보 보호 적용 설계 원칙에 따르면, 우선 개인정보 수집을 제한하는 등의 GDPR에서 규정한 원칙을 준수하는 방식으로 사업 프로세스를 설계해야 한다. 개인정보 흐름을 최소화하고 가능한 경우 익명처리 등을 통해 개인정보 처리를 방지할 수 있게 프로세스를 설계해야 한다. 개인정보 보호 적용 설계 원칙은 개발 프로세스를 시작할 때부터(예를 들면 보호조치를 구현하기 위해 IT 개발회사와 함께) GDPR에 규정된 권리를 고려할 것을 기업에 요구한다.

개인정보 보호 기본 설정 원칙은 기본적으로 처리의 구체적인 목적을 위해 필요한 개인정보만 처리하도록 하기 위해 적절한 기술적이고 관리적인 조치를 취할 것을 컨트롤러에게 요구한다. 개인정보 보호 적용 설계 원칙과 유사하게, 개인정보 보호 기본 설정 원칙은 개인정보 보호에 대한 자문을 구하고 개발 프로세스의 초기 단계에 개인정보 보호에 친화적인 서비스의 사전 설정을 통해 개인정보의 처리 정도를 합리적으로 제한하고 보유 기간을 단축하며 가능한 한 열람 가능성을 제한하도록 설계할 것을 컨트롤러에게 요구한다. 따라서 개인정보 보호는 기본 설정 사항이 되어야 한다!

3.7 개인정보 보호 영향 평가(Privacy Impact Assessment) - 정의 및 실시 여부 평가

GDPR이 도입한 또 다른 예방 메커니즘에 따르면 컨트롤러는 “개인정보 보호 영향 평가(PIA)”를 실시해야 한다. 이는 계획된 절차를 도입하기 전에 해당 절차가 GDPR을 준수하는지를 사전에 평가, 보장 및 문서화하는 것이다. 자연인의 권리와 자유를 침해할 가능성이 큰 구체적인 경우, 특히 새로운 기술을 사용하여 개인정보를 처리하는 경우에는 개인정보 보호 영향 평가를 실시해야 한다.

컨트롤러가 다음을 수행하는 경우, 개인정보 보호 영향 평가를 실시해야 한다.

- (i) (a) 프로파일링을 포함하는 자동화된 처리에 기초하여 자연인의 개인정보를 체계적이고 광범위하게 평가하고 (b) 이런 평가에 기초하여 결정하고 (c) 자연인에 대하여 법적 효과를 발생시키거나 자연인에 대하여 상당한 영향을 미치는 처리 활동을 의미하는 자동화된 의사결정과 프로파일링을 포함하는 절차(예: 자동화된 처리에 기초한 신용 평가와 신용평가에 기초하여 대출 계약을 자동적으로 거부하는 것)
- (ii) GDPR 제9조 제(1)항에서 언급하는 민감정보(예: 건강에 대한 개인정보)나 GDPR 제10조에서 언급하는 범죄경력 및 범죄행위와 관련한 개인정보를 대규모로 처리하는 경우.
- (iii) 공개적으로 열람할 수 있는 곳(예: CCTV설치 장소)을 대규모로 체계적으로 모니터링하는 경우.

유럽의 개인정보 감독기구는 여러 지침과 함께 관련 사례에 대한 논평을 발표하였으며 이를 계속 업데이트한다. 따라서 개인정보 보호 영향 평가의 실시 여부에 상관없이 평가를 수행할 때는 이러한 지침과 논평을 고려해야 한다.

■ 예시

- 프로파일링(신용 조사나 대출 신청과 같은 정보주체의 개인정보에 기초한 자동화된 의사결정)과 관련된 모든 정보처리 활동
- 클라우드 컴퓨팅이나 빅 데이터와 같은 혁신적인 기술의 사용
- GDPR 제9조와 제10조에 따른 개인정보의 대규모 처리(예: 정당 가입 관련 개인정보, 병원, 체육관, 보건소가 처리하는 건강 관련 기록, 데이터 주선 웹사이트/신청)
- 공개적으로 열람할 수 있는 장소(예: 전시장 또는 이와 유사한 곳)에 대한 체계적인 대규모의 모니터링(예: CCTV를 통한 모니터링)
- 임직원의 행동에 대한 모니터링

개인정보 보호 영향 평가를 실시해야 하는 경우, 개인정보 보호 영향 평가는 다음 사항을 포함하고 문서화해야 한다.

- (ii) 설계 중인 정보처리 작업과 처리 목적에 대한 체계적인 설명(가능한 경우 컨트롤러가 추구하는 적법한 이해를 포함)
- (iii) 목적과 관련한 처리 작업의 필요성과 비례성에 대한 평가
- (iii) GDPR의 관련 조항에서 언급하는 정보주체의 권리와 자유에 대한 위협의 평가
- (iv) 위협을 다루도록 설계 중인 조치(정보주체와 다른 관계자의 권리와 적법한 이익을 고려하여 개인정보를 보호할 것을 보장하고 GDPR을 준수하는 것을 입증하는 보호조치, 보안 조치 및 메커니즘을 포함)

프로세서는 일반적으로 컨트롤러를 대신하여 운영하는 절차에 대하여 개인정보 보호 영향 평가를 실시할 필요가 없다. 하지만 임직원이 문제의 개인정보를 처리하는 경우, 개인정보 보호 영향 평가를 실시해야 할 수도 있다.

결과적으로, 개인정보 보호 영향 평가를 실시해야 하는지를 결정하기 위해 다음과 같은 기본적인 사항을 확인할 수 있다.

■ 체크리스트

- 정보처리 활동에 대한 목록을 검토하고 위험도가 높은 처리 활동을 찾는다.
- 위험도를 평가하기 위해 개인에 대한 영향의 가능성과 정도를 고려해야 한다(낮은 수준의 피해가 발생할 가능성이 크거나 심각한 피해가 발생할 가능성이 적은 경우, 위험도가 클 수 있다).
- 개인정보 보호 영향 평가는 다음을 포함해야 한다.
 - 처리의 성격, 범위, 맥락 및 목적에 대한 설명
 - 필요성, 비례성 및 준수 조치에 대한 평가
 - 개인에 대한 위협의 확인 및 평가
 - 이러한 위협을 완화하기 위한 추가 조치의 확인
- 모든 단계를 철저하게 문서화한다.

4 정보주체의 권리 보장을 위한 우리 기업의 조치사항은 무엇인가?

법적 근거에 기초하여 개인정보를 처리하고 적법한 처리 원칙을 준수하더라도 정보주체가 권리를 행사하는 경우, 정보주체의 요청에 즉시 응해야 한다.

그 이유는, GDPR이 정보주체의 권리를 강화하고 의식을 고취시켰기 때문이다. 예를 들어, 사업 관계나 고용 관계가 종료된 후 GDPR에 의거하여 더 많은 고객이나 임직원이 자신의 개인정보를 열람하거나 파기할 것을 요청하는 사례가 늘어날 것이다.

개인정보 처리 및 관련 시스템은 정확성을 보장하는 옵션을 제공하여야 하며, 법적으로 필요한 경우에는 이에 따라 개인정보를 수정하는 간편한 방법을 제공해야 한다.

각 요청에 대응할 수 있기 위해 기업은 합리적인 시간 내에 이러한 요청에 대응하고 이 요청을 준수할 수 있는 절차와 기술적 및 관리적 조치를 결정해야 한다. 이런 권리는 자유롭게 행사할 수 있으며 일반적으로 30일 내에 충족시켜야 한다.

4.1 열람권(Right to Access)

GDPR은 제15조에서 열람권을 규정한다. 열람 요청을 받는 경우, 특정 개인에 대한 개인정보를 보유하고 있는지를 확인하고 열람 요청을 한 사람에게 이를 통지할 수 있어야 한다(단계 1). 특정 개인에 대한 개인정보를 보유하고 있으며 열람 요청을 한 사람에게 이를 통지할 수 있는 경우, 정보주체는 다음 정보를 추가로 요청할 수 있다(단계 2).

- 개인정보의 사본(예: 정보주체에 대하여 귀사가 보유하고 있는 개인정보의 목록을 제 공함으로써)
- 개인정보의 처리 목적, 범주 및 보유 기간과 같은 추가적인 “메타 데이터(metadata)”
- 정보주체의 삭제권, 정정권 및 제한권에 대한 정보
- 감독기구에 민원을 제기할 권리
- 개인정보의 출처(예: 웹사이트 등) 대한 정보
- 개인정보의 제3자 이전에 대한 정보
- 자동화된 의사결정을 사용하는 경우
- 개인정보의 수령인에 대한 정보

이런 정보를 제공하는 것과 관련하여 특정한 방식이 있는 것은 아니다. 하지만 결국 GDPR을 준수하는 것을 입증하기 위해서는 공개한 개인정보를 적절하게 문서화할 것을 권장한다.

법률에 따라 매우 짧은 시간 내(일반적으로 단계 1의 경우 약 4주, 그리고 단계 2의 경우 4 주부터 8주까지)에 요청에 응답해야 한다는 사실을 고려할 때 개인정보를 찾고 정보주체 에게 이를 적절하게 공개하는 프로세스를 구축해야 한다.

요청 당사자가 승인되는지 여부를 평가하기 위한 시간이 필요할 수 있다는 점을 명심해야 한다. 따라서 승인되지 않은 개인에게는 개인정보를 공개하지 않도록 해야 한다.

4.2 삭제권(Right to Erasure), 정정권(Rectification), 제한권(Restriction) 보장

GDPR 제16조, 제17조 및 제18조에서 규정한 이들 권리는 컨트롤러가 법률을 위반하는 것을 방지하거나 취소하기 위한 것이다. 이들 권리는 정보주체에게 가장 효과적인 권리 이다. 개인정보를 적법하게 수집하고 처리한 경우 또는 목적을 생략한 경우, 삭제권을 적 용한다. 정정권은 정확성의 원칙을 명시하며, 처리한 개인정보는 현실을 반영해야 한다.

GDPR 제18조에서 규정한 정보처리의 제한권은 컨트롤러의 이익과 정보주체의 이익 사이에서 균형을 유지하기 위한 것이다.

일반적으로 삭제권은 적법한 방식으로 요청하는 경우, 개인정보를 완전히 삭제할 것을 컨트롤러에게 요구한다. 단순히 개인정보를 차단하는 것은 GDPR 제17조를 준수하기에 충분한 조치가 아닐 수 있다.

■ 체크리스트

- ☑ 삭제 요청을 효과적으로 준수하기 위한 프로세스를 수립해야 한다.
- ☑ 삭제 요청을 적시에 적절하게 다루는 방법에 대해 임직원을 교육한다.
- ☑ 요청을 충족시키기 위하여(즉 개인정보를 확인하고 필요한 경우, 이를 적절하게 삭제하는) 시스템을 수립한다.

4.3 이동권(Right to Data Portability) 보장

GDPR 제17조에 따른 개인정보 이동권은 정보주체의 권리에 대한 여러 획기적인 보호조항 중 하나이다. 이 권리는 정보주체의 개인정보를 한 컨트롤러로부터 다른 컨트롤러에게로 이전할 수 있도록 하기 위한 것이다. 이 권리의 목적은 컨트롤러가 경제적 상황에 더 잘 적응할 수 있도록 하고 개인정보를 처리하는 서비스 제공업체들 간에 경쟁을 촉진하는 것이다. 하지만 이 권리는 하나의 법률이 아니라 여러 의무와 주장을 하나로 묶은 것이다. 정보주체는 개인정보를 수령할 수 있는 권리와 자신의 개인정보를 특정한 포맷으로 전송하도록 지시할 수 있는 권리가 있다. 이 권리와 관련하여 다음과 같은 네 가지의 누적조건을 충족해야 한다. 즉, 정보주체의 개인정보를 처리해야 한다. 이러한 처리를 자동화하며, 정보주체는 동의나 계약에 기초하여 개인정보를 제공해야 한다.

이 권리에 따라 제공 가능한 개인정보와 제공 불가능한 개인정보를 구별하는 것은 사실 매우 어렵다. 고객이 서비스 제공업체를 주기적으로 변경하고 새로운 업체의 서비스를 이용

하기 위해 개인정보를 가져가고자 할 가능성이 많은 사업 분야에 종사하는 경우, 이런 권리를 더 자세하게 평가해야 한다. 개인정보 이동권과 관련한 세부사항에 대하여 여전히 논의가 진행 중이라는 점도 유의해야 한다.

따라서 이 권리와 관련한 새로운 전개 사항을 면밀하게 관찰해야 한다!

4.4 반대권(Right to Object) 보장

GDPR 제6조 제(1)항 제(e)호와 제(f)호에 따라 적법하게 처리하는 경우(적법한 이익에 기초한 대부분의 경우), GDPR 제21조에 따른 반대권이 정보주체의 특별한 이익을 보호한다. 정보주체가 반대권을 행사하는 경우, 정보주체가 개인정보의 처리를 불법화하는 특정한 상황과 관련한 근거를 제시하면 처리를 종료하고 개인정보를 삭제해야 한다. 하지만 컨트롤러가 개인정보를 계속 처리하는 것에 대한 적법한 근거(정보주체의 이익, 권리 및 자유에 우선하는) 입증하는 경우, 또는 사업장이나 법적 권리를 행사하거나 보호하기 위하여 처리가 필요한 경우에는, 컨트롤러는 개인정보를 계속해서 처리할 수 있다.

컨트롤러가 직접 마케팅을 위해 개인정보를 사용하는 경우, GDPR 제21조 제(2)항은 개인 정보의 처리에 대한 법적 근거에 상관없이 반대권을 부여한다. 따라서 컨트롤러는 이러한 요청을 준수해야 한다. 많은 국가에서 이러한 접근법을 채택하고 있다.

■ 체크리스트

- 정보주체의 반대권에 대해 숙지한다!
- 정보주체의 권리를 보장하는 메커니즘을 정보주체의 요청에 따라 적절한 때에 구현한다!
- 이에 따라 임직원을 훈련시킨다!
- 정보주체의 요청을 무시하지 않는다. 그렇지 않으면 다루기 어려워질 수 있다!

5 기업의 책임성은 무엇이며, 문서화 요건을 어떻게 해야 충족시키는가?

“법적 근거”에 기초하여 개인정보를 처리하고 개인정보의 적법한 처리에 대한 원칙을 준수하는 경우, 적용 가능한 법률을 준수하는 것에 대한 증거(“책임성”)를 제공해야 한다.

감독기구가 요청하는 경우, 컨트롤러는 입증 책임을 지며, GDPR을 준수하는 것을 입증할 수 있어야 한다. 법률에 따른 처리 활동에 대한 컨트롤러의 기록이 도움이 될 것이며 이런 기록은 기업의 개인정보 흐름에 대한 세부 사항을 포함해야 한다. 해당 기록은 서면이나 전자적 형태로 보관되어야 하며, 감독기구가 요청하는 경우, 이런 기록을 제공해야 한다.

컨트롤러의 처리 활동에 대한 기록은 처리 활동과 관련하여 다음과 같은 기본적인 정보를 표시해야 한다.

- 컨트롤러와 해당하는 경우 공동 컨트롤러, 컨트롤러 대리인 및 DPO의 이름과 연락처 정보
- 정보처리 목적
- 정보주체의 범주와 개인정보의 범주에 대한 설명
- 개인정보 수령인(제3국에 있는 수령인과 국제기구를 포함)의 범주
- 제3국 또는 국제기구로의 개인정보 이전 및 제49조 제(1)항 제(b)호에 명시된 이전의 경우, 적절한 보호조치에 대한 문서화
- 가능한 경우, 서로 다른 범주의 개인정보를 삭제하는 데 대한 시간제한
- 가능한 경우, 제32조 제(1)항에서 언급하는 기술적 및 관리적 보안 조치에 대한 일반적인 설명

프로세서의 처리 활동에 대한 기록도 위에서 설명한 것과 유사한 정보와 다음 정보를 표시하여야 한다.

- 프로세서, 컨트롤러를 대신하여 행동하는 프로세서, 컨트롤러나 프로세서의 대리인 및 DPO의 이름과 연락처 정보
- 각 컨트롤러를 대신하여 수행하는 개인정보 처리의 범주
- 제3국 또는 국제기구로의 개인정보 이전(제3국이나 국제기구의 식별을 포함하는) 및 제49조 제(1)항 제(b)호에 명시된 이전의 경우, 적절한 보호조치에 대한 문서화
- 가능한 경우, 제32조 제(1)항에 명시된 기술적 및 관리적 보안 조치에 대한 일반적인 설명
- 제32조 제(1)항에서 언급하는 보안 조치

정보처리 활동에 대한 기록 유지 의무는 특히 중소기업의 경우에 많은 자원과 시간을 소모할 수 있기 때문에, GDPR은 이러한 기록 유지부로부터 회사를 면제하는 것에 대하여 최소 기준을 규정한다. GDPR 제30조 제(5)항에 따르면 250명 미만을 고용하는 기업이나 조직은 기록부를 유지해야 하는 의무가 없다. 단 해당 기업이나 조직이 수행하는 정보처리가 정보주체의 권리와 자유를 침해할 위험이 있는 경우이거나 간헐적인 개인정보 처리가 아닌 경우, 또는 GDPR 제9조 제(1)항에서 언급하는 민감정보나 전과나 범죄에 대한 개인정보를 처리하는 경우는 제외한다.

요약하면, 조직의 규모와 관계없이 민감한 개인정보 처리 활동을 수행하는 경우에는 기록부를 유지해야 한다.

또한 처리 활동에 대한 기록부는 더 발전한 개인정보 보호 관리 시스템(Data Protection Management System, DPMS)의 핵심 요소 중 하나이며, 적합한 경우 개인정보 보호 관리 시스템을 구현해야 한다. 개인정보 보호 관리 시스템은 내부 준수 시스템이며, 기존의 준수 시스템에 기초하거나 기존의 준수 시스템과 결합하여 기존의 절차를 간소화할 수 있다.

개인정보의 처리에 대한 사항을 GDPR에 따라 문서화하는 방법과 관련하여 먼저 다음 체크리스트를 참고하여야 한다.

■ 체크리스트

- ☑ 개인정보 보호 준수에 따라 포함한 결정과 프로세스를 광범위하게 문서화한다.
- ☑ GDPR 제30조와 규제기구가 제공하는 샘플/모범사례를 사용하여 문서화한 결과를 검토한다.
- ☑ 처리 모니터링하고 이를 최신 상태로 유지하기 위한 메커니즘과 절차를 구현한다.
- ☑ 워크숍, 훈련, 등을 통해 개인정보 보호에 대한 인식을 강화한다.
- ☑ 필요한 경우, DPO나 변호사에게 도움을 요청한다.

6 기술적 · 관리적 조치(Technical and Organisational Measure)는 어디까지?

GDPR 제32조는 개인정보를 보호하기 위하여 적절한 기술적 및 관리적 조치(technical and organisational measures, TOM)를 취할 것을 컨트롤러와 프로세서에게 요구한다. 따라서 개인정보 처리의 성격, 범위, 맥락 및 목적 그리고 개인의 자유와 권리에 대한 위험을 고려해야 한다. 위에서 설명한 바와 같이 법률은 개인정보 보안과 관련하여 위험에 기반한 접근법을 활용할 것을 요구하며 기술적 · 관리적 조치가 개별 상황에 따라 적절한지를 이해 관계자가 평가할 것을 요구한다.

GDPR은 정보주체나 기타 관련 당사자에 대한 잠재적 위험을 줄이기 위해서 취해야 하는 조치를 다음과 같이 명시하고 있다.

- (i) 개인정보의 가명처리 및 암호화
- (ii) 처리 시스템과 서비스의 기밀성, 무결성, 사용 가능성 및 유연성을 계속 보장할 수 있는 능력
- (iii) 물리적 또는 기술적 사건이 발생하는 경우, 개인정보의 사용 가능성과 열람을 적시에 회복할 수 있는 능력
- (iv) 처리의 보안을 보장하기 위하여 기술적 · 관리적 조치를 정기적으로 검사, 사정 및 평가하는 프로세스

GDPR은 매우 일반적인 표현으로 이를 규정하기 때문에, 많은 기업은 실제로 무엇을 해야 하는지 고심하고 있다. 일상적인 업무에서 취하는 가장 일반적인 조치 중 일부는 다음을 포함한다.

- 인가되지 않은 사용자의 경우, 개인정보 처리 시스템을 사용하지 못하도록 한다(예: 적합한 비밀번호 사용).
- 개인정보 처리 시스템을 사용할 수 있는 권리가 있는 사람은 열람권이 있는 개인정보만 열람할 수 있도록 한다(예: 접근 관리 시스템 사용).
- 처리 중 또는 전자적으로 전송하는 중에 인가 받지 않은 개인정보 열람, 복사, 수정, 제거를 제한한다(예: 개인정보 암호화).
- 개인정보를 개인정보 처리 시스템에 입력하거나 수정하거나 제거하였는지를 확인하고 결정할 수 있어야 한다(예: 파일 프로토콜).
- 개인정보를 우발적으로 파괴하거나 상실하는 것으로부터 개인정보를 보호 해야한다(예, 백업, 재난 복구 계획 등).

법률이 요구하는 바는 정보처리에 의해 발생하는 위협의 정도에 따라 다르다. 예를 들어 민감정보의 경우에, 발생하는 위협의 정도는 더 클 수 있다.

평가로 인해 도출된 결론을 개인정보 보호 개념에 적용하여야 한다. 이를 통하여 처리 활동의 중요성에 따라 개인정보 처리 활동을 분류하고 접근법을 문서화하여 개인정보의 보안과 무결성을 적절한 수준으로 보장할 수 있다.

보안 개념과 이를 준수하는 방법을 입증하기 위해, 정기적 교육과 워크숍을 통해 임직원의 인식을 개선하고, 정기적으로 관리하고 시험하도록 한다. 이를 통해 조치의 질과 효과를 적절하게 유지한다.

7 개인정보 보호 책임자(DPO) 선임이 필요한 경우는 언제인가?

정보처리의 종류와 개인정보의 범주에 따라 개인정보 보호 책임자를 지정해야 할 수 있다.

7.1 개인정보 보호 책임자의 역할

개인정보 보호 책임자의 직무는 GDPR 제39조에 명시되어 있으며, 최소한 다음을 포함한다.

- GDPR에 따른 의무를 임직원에게 을 통지하고 이를 관리할 것을 권고한다.
- 모든 개인정보 보호 조항을 준수하는지 모니터하고 개인정보 보호 정책을 수립한다(처리 작업 및 회계 감사와 관련한 책임의 부여, 인식의 개선 및 교육 포함).
- 정보주체 및 감독기구와 협력하고 소통하는 것을 관리한다.

개인정보 보호 책임자는 독립적이어야 하고 최고 경영진에만 보고한다. 또한 개인정보 보호 책임자는 개인정보 보호 분야의 전문가여야 하며 직무를 적절하게 수행할 수 있어야 한다. 개인정보 보호 책임자는 내부 직원 중에서 지정할 수 있으며, 외부에서 고용할 수도 있다.

7.2 개인정보 보호 책임자 지정 의무가 있는 기업 유형

GDPR에 의거하여, 직원이 250명 이상인 기업의 경우 일반적으로 개인정보 보호 책임자를 지명해야 한다. 하지만 다음 경우에는 개인정보 보호 책임자를 반드시 지명해야 한다.

- (1) 핵심 활동이 개인정보의 처리이며 처리의 성격, 범위 또는 목적에 따라 대규모의 정보 주체를 정기적이고 체계적으로 모니터링 해야 하는 경우(예: 비디오 감시나 인터넷 추적), 또는
- (2) 핵심 활동이 대규모의 민감정보 처리인 경우(예: 건강 관련 개인정보)

또한 현지 법률은 일반적으로 회사의 규모에 따라 개인정보 보호 책임자를 지정해야 하는 상황을 규정할 수 있다(예: 독일의 경우, 현재 10명 이상의 직원을 고용한 회사는 개인정보 보호 책임자를 지정해야 하며 새로운 법률을 제정하는 경우 새로운 기준을 규정할 수 있다).

기업의 조치에 따른 책임을 개인정보 보호 책임자가 인수하지 않는다는 점을 유념해야 한다 (일반적인 민법, 고용법, 불법행위에 대한 법률에 따른 경우는 제외한다). 개인정보 보호 책임자는 개인정보의 보호와 관련한 회사의 조치를 관리할 뿐이다. 귀사는 적절한 자원을 개인정보 보호 책임자에게 제공해야 한다. 또한 사업과 관련한 귀사의 결정이 개인정보 보호에 영향을 미치는 경우, 개인정보 보호 책임자로 하여금 이에 참여하도록 해야 한다.

한국 기업과 관련하여 중요한 점은 다음과 같다. 한국 내에 있고 GDPR의 적용 대상인 기업의 경우, 개인정보 보호 책임자를 지정해야 한다는 점이다. 사업장의 위치에 관계없이 개인정보 보호 책임자를 지정하여야 한다.

■ 체크리스트

- ☑ GDPR이나 국가 법률에 따라 개인정보 보호 책임자를 지정해야 하는지 확인한다. 일부 국가에서는 개인정보 보호 책임자 지정과 관련 규칙이 더 엄격하다. 개인정보 보호 책임자를 지정해야 하는지 확실하지 않은 경우, 이에 대해 변호사에게 확인해야 한다.
- ☑ 필요한 경우, GDPR의 규정을 충족하는 개인정보 보호 책임자를 지정한다.
- ☑ 개인정보 보호 책임자 지정 관련 사항을 적절하게 문서화한다.
- ☑ 개인정보 보호 책임자가 귀사의 조직을 지원할 수 있도록 하며, 개인정보 보호 책임자를 배제하지 않는다.

8 개인정보의 EU 국외 이전 등 제3자에게 제공하는 경우

개인정보의 외부 흐름을 관리하는 경우, 앞에서 설명했듯이 개인정보를 제3자에게 이전하는 것은 개인정보를 “처리”하는 것으로 간주한다는 점을 유념해야 한다. 이는 기업에 속하지 않는 제3자에 대한 개인정보 이전은 모두 투명하고 법적 근거에 기초해야 함을 의미한다. 개인정보를 계속 관리하면서 제3자가 이를 열람할 수 있도록 하는 것도 이전으로 간주된다는 점에 유의해야 한다. 아래 예시는 이에 대한 상세한 사항을 설명한다.

8.1 그룹 내부에서 이전하는 경우

이 경우, 제3자는 그룹에 속하는 회사도 포함한다. 이는 법률이 그룹 내부에서 개인정보를 자유롭게 이전할 수 있는 일반적인 특권을 규정하지 않기 때문이다(그룹 내부 특권 없음). 따라서 그룹 내의 각 기업은 개인정보 보호에 대한 책임을 지낸다.

그룹 내에서 개인정보를 이전하기 위해서는 몇 가지 대표적인 조치와 보호조치를 통해 GDPR을 준수해야 한다. 가장 대표적인 조치는 그룹 내에서 개인정보 처리 계약을 체결하는 것이다(아래 참조). 또한 관리 지원 등과 관련한 경우, GDPR은 그룹 내에서 개인정보를 이전하는 것에 대해 일부 특권이 존재한다는 점을 인정한다. 그 경계를 아직 명확하게 규정하지는 않았지만 그룹 내 이전이 최소한 어느 정도까지는 적법한 이익에 기초한다는 주장이 제기되었다(GDPR 제6조 제(1)항 제(f)호 참조). 이러한 문제에 직면하는 경우, 보호조치를 정의하기 위해 개인정보 보호 책임자와 변호사로부터 전문적인 자문을 얻어야 한다.

8.2 프로세서에게 이전하는 경우

컨트롤러를 대신하여 컨트롤러의 IT 시스템을 운영하거나 특정한 소프트웨어 제품을 유지 관리하고 지원하는 호스팅 서비스 제공업체와 같은 개인정보 프로세서는 개인정보보호 법률의 관점에서 컨트롤러 조직의 일부로서 간주된다. 따라서 개인정보 프로세서에게 개인정보를 이전하는 경우, 정보주체의 동의와 같은 별도의 법적 근거가 필요하지 않다.

하지만 프로세서로서 개인정보 사용에 대한 주요 요건은 GDPR 제28조에 따라 개인정보 처리 계약을 체결하는 것이다(세부 사항에 대해서는 상기 제2절 참조).

8.3 EU/EEA 국외 이전하는 경우

다른 쟁점은 EU/EEA 역외로 개인정보를 이전하는 것이다. 다시 말해서, 개인정보 보호조치가 적절하지 않은 국가로 개인정보를 이전하는 것이다. 이러한 경우, GDPR은 개인정보 보호에 대한 최소한의 기준을 보장하기 위해 적절한 대안을 활용하도록 요구한다.

GDPR은 이를 달성할 수 있는 여러 가지 방법을 규정한다. 특정 국가를 GDPR 제45조(적정성 결정)에 따른 안전한 국가로 간주하는 경우, 해당 국가로 개인정보를 이전하는 데 있어 이미 위에서 설명한 조치(예: GDPR 제5조와 제6조의 준수) 이외의 별도의 조치는 필요하지 않다. 요약하면 GDPR 제6조에 따른 유효한 법적 근거가 있는지 그리고 GDPR이 개인정보의 역외 이전과 관련하여 규정한 추가 요건(GDPR 제44조)을 준수하는지 여부를 항상 확인해야 한다.

다음 예시는 이를 보여준다.

■ 예시

귀사는 유럽 기업으로서 한국 내에 있는 서비스 제공회사로부터 IT 유지 보수 서비스를 받고 있다. 이 서비스 제공회사는 귀하의 고객에 대한 개인정보를 열람할 수 있다. 이 서비스 제공회사를 프로세서로 간주한다. 따라서 개인정보 처리 계약을 체결해야 한다(GDPR 제28조 참조). 또한 서비스 제공회사가 역외에 위치한 국가(EU 집행위원회(European Commission)로부터 아직 적정성 결정을 받지 않은)에 있기 때문에 개인정보 처리 계약에 더하여 GDPR 제44조에 따른 다른 조치(예: 표준 개인정보보호 조항 체결 등)가 필요하다.

대표적으로 사용되는 수단은, EU 표준 개인정보보호 계약(standard contractual clauses)이다. 이는 EU 집행위원회가 역외 개인정보 이전에 대한 계약에 포함하도록 고안한 일련의 모델 조항이다. 다른 옵션은 구속력이 있는 기업 규칙이다. 이는 유럽의 규제기구가 역외 개인정보 이전을 포함하기 위해 협의 및 승인한 계약이다.

역외 개인정보 이전을 포함하는 여러 다른 옵션을 검토하는 경우, 다음과 같은 질문을 고려해야 한다.

■ 제3국 이전

- 적정성 결정 국가로 이전하는가? (예: 이스라엘, 캐나다) 미국에 대한 프라이버시 실드 인증(Privacy Shield Certification)이 이 범위에 해당한다는 것에 주의해야 한다.
- 적정성 결정 국가로 이전하는 것이 아닌 경우, 역외 이전을 합법화하기 위해 EU 집행위 원회가 규정하는 모델인 표준 개인정보보호 계약을 체결할 수 있는가? 표준 개인정보보호 계약을 체결할 수 있는 경우, 이는 대표적이고 가장 현실적인 솔루션이다.
- 표준 개인정보보호 계약을 체결할 수 없는 경우, 관할 감독기구가 인정하는 특별 계약이 있는가?
- 구속력이 있는 현행 기업 규칙이 다른 대안이 될 수 있다. 이러한 규칙이 있는가?

일반적으로 경우, EU/EEA의 역외에 있는 프로세서와 관련이 있는 경우, 대부분의 회사는 개인정보 이전을 포함하도록 상기 표준 개인정보보호 계약을 체결하는 것을 목표로 한다. 개인정보의 이전을 포함하도록 상기 표준 개인정보보호 계약을 사용하는 경우, 여러 모델 조항이 있으며 이를 EU 집행위원회의 웹사이트에서 확인할 수 있다는 것을 고려한다. 이 중 일부는 “컨트롤러 간” 이전에 해당한다. 따라서 역외 프로세서와 관련이 있는 경우, 이는 올바른 선택이 아니다. 어떤 종류의 문서가 귀사의 상황과 맞는지 DPO와 변호사에게 문의한다.

9 GDPR의 법적 구속력

- 개인정보를 보호하기 위해 무엇을 해야 하는지에 대한 개요를 위에서 설명하였다. 아래에서는 개인정보 보호를 준수하지 않는 경우, 어떤 결과가 발생하는지를 설명한다.
- 개인정보 보호 규정과 관련 의무를 준수하지 않는 경우, 책임 및 처벌의 대상이 될 수

있다. 한 국가 내에서의 책임 및 처벌의 종류는 법률을 통해 예상할 수 있다. 일반적으로 책임 및 처벌은 다음으로 구성된다.

- 민사 책임(정보주체에 대한 민원이나 집단 소송에 따른)
- 형사 책임(벌금, 구금 등)
- 행정상 책임(주의와 과징금 등의 행정 조치)
- 회사의 평판 훼손

GDPR을 위반할 경우, 최고 2,000만 유로의 과징금과 사업체의 경우, 직전 회계 연도에 대한 그룹의 전세계 연간 매출액의 최고 4%에 해당하는 과징금 중 더 큰 금액에 대한 과징금이 부과될 수 있다는 점을 유념한다.

과징금은 개별 사례에 따라 달라질 수 있다. 각 개별 사례에서 과징금 부과 여부를 결정하고 과징금 금액을 결정하는 경우, 개인정보 감독기구는 다음 기준을 적절히 고려해야 한다.

- (i) 위반의 성격, 심각성 및 기간, 정보처리의 성격, 범위 또는 목적 및 처리에 따라 영향을 받는 정보주체의 수
- (ii) 위반의 고의성이나 과실 여부
- (iii) 정보주체의 손해를 완화하기 위하여 컨트롤러나 프로세서가 취하는 조치
- (iv) 컨트롤러나 프로세서가 제25조와 제32조에 따라 취하는 기술적·관리적 보호조치를 고려한 컨트롤러나 프로세서의 책임 정도
- (v) 컨트롤러나 프로세서의 과거 위반 사항
- (vi) 위반 사항을 구제하고 위반으로 인한 악영향을 완화하기 위하여 감독기구와 협력하는 정도

상기 목록은 관계 기구와 건설적으로 협력하고 GDPR을 준수하는 것이 얼마나 중요한지를 보여준다.

10 감독기구와 협력

관련 감독기구가 요청하는 경우, GDPR 제31조에 따라 관련 감독기구와 협력해야 한다. 하지만 각 EU 회원국에는 감독기구가 있고(일부 회원국에는 감독기구가 여러 개 있으며, 독일의 경우 17개의 개인정보 감독기구가 있다), 오늘날에는 처리 활동이 여러 국가에 걸쳐 발생하기 때문에(여러 다른 EU 회원국에서 발생하고 여러 다른 나라의 국민에게 영향을 미치기 때문에) 관할 감독기구를 결정하는 것이 어려울 수 있다.

감독기구는 GDPR 제58조에서 규정하는 조사 및 정정 권한을 가진다. 필요한 경우, 감독기구는 개인정보 보호를 위한 감사를 실시하며, 이를 위해 필요한 모든 정보와 개인정보를 열람할 수 있다.

또한 감독기구는 각 개별 사례의 상황에 따라 GDPR에 명시된 조치에 더하여, 또는 이를 대신해서 문제의 처리 활동이 GDPR의 조항을 위반하거나 과징금을 부과할 가능성이 있다는 것을 컨트롤러나 프로세서에게 경고할 수 있다.

GDPR 제56조 제(6)항에 따라 선임 감독기구(Lead Supervisory Authority)는 처리 활동이 여러 EU 회원국에 영향을 미치는 컨트롤러나 프로세서에 대한 유일한 접촉점의 역할을 해야 한다. 따라서 회사의 주요 사업장의 위치를 선택하는 경우, 선임 감독기구도 자동적으로 선택된다. 국가의 감독기구가 얼마나 엄격한지에 따라 주요 사업장의 위치를 선택하는 것에 영향을 미칠 수 있다. 한 국가에 있는 회사의 특정한 지사나 사업장에서만 특정 개인정보 처리 활동을 하는 경우, 이러한 일괄처리 “One-Stop-Shop” 절차가 적용되지 않는다는 사실을 유념해야 한다. 이 경우, 특정 국가에 있는 감독기구가 관할권을 가진다.

■ 체크리스트

- 감독기구와의 연락 책임이 있는 한 명을 지명함으로써 감독기구와 협력해야 하는 의무를 항상 준수한다.
- 여러 국가가 관련된 경우, 어느 감독기구가 단일 접촉점이 될 것인지를 확인한다.
- 이러한 직무를 효과적으로 수행하기 위한 메커니즘을 구축 및 교육한다.

11 개인정보 침해 시 대응 조치

개인정보에 대하여 불법적 또는 우발적으로 다음 행위를 할 경우, 개인정보 침해가 발생한다.

- 파기 또는 소실(예: 직원 파일 삭제, 개인정보 매체 손상, 노트북 도난, 사업용 핸드폰 분실)
- 변경(예: 마스터 개인정보 조정, 특정 개인정보 필드의 우연한 삭제, 파일 손상)
- 노출(예: 잘못 보낸 이메일, 원격 접속의 우연한 활성화, 임직원 파일 무단 열람)

일반적으로 개인정보 침해 발생 후 72시간 안에 관할 EU 개인정보 감독기구에 해당 사실을 통지해야 한다. 컨트롤러는 이러한 의무를 이행해야 한다.

통지 내용에는 다음 내용을 포함해야 한다.

- (i) 개인정보 침해의 성격(가능한 경우, 해당 정보주체의 범주 및 그 수의 추정치, 해당 개인정보 기록의 범주 및 그 수의 추정치 포함)
- (ii) 더 상세한 정보를 제공할 수 있는 DPO 또는 다른 접촉점의 이름과 연락처 정보
- (iii) 개인정보 침해로 인해 발생 가능한 결과
- (iv) 개인정보 침해에 대하여 컨트롤러가 취하거나 취하도록 제안하는 조치(적절한 경우, 발생 가능한 악영향을 완화하는 조치 포함)

프로세서는 컨트롤러가 자신의 의무를 준수할 수 있도록 하기 위해 이러한 활동에 대해 컨트롤러에게 즉시 적절하게 통지해야 한다(GDPR 제33조 참조).

참고: 개인정보 침해가 주말이나 공휴일에 발생하는 경우에도, 72시간의 통지 유효 기간은 연장되지 않는다. 따라서 침해를 감지하는 경우, 시간 준수가 가장 중요하다!

개인정보 침해가 자연인의 권리와 자유에 위협을 초래할 가능성이 있는 경우(예: 정보주체에 대한 손해가 임박한 경우), 컨트롤러는 개인정보 침해 사실을 정보주체에게 즉시 통지해야 한다. 일반적으로 이러한 통지를 하지 않는 것이 해당 회사의 이익에 부합할 수 있으나, 침해의 범위에 따라 종종 이를 관리하기 어렵다. 따라서 어떠한 경우에도 즉시 통지해야 한다.

개인정보 침해를 감지하거나 의심하는 경우, 책임이 있는 이해당사자에게 즉시 통지해서 필요한 조치를 취할 수 있도록 한다. 회사는 이런 상황에 적절하게 대처하는 위한 효과적인 절차를 수립하고 책임을 규정하며 이를 적절하게 문서화해야 한다.

대응팀이 개인정보 침해 사건에 얼마나 적절히 대응하고 손해를 최소화할 수 있는지는 해당 기업에 대한 벌금 및 처벌에 큰 영향을 미칠 것이다.

개인정보 침해에 적절하게 대응하기 위해 다음 체크리스트가 도움이 될 수 있다.

■ 체크리스트

- 대응 계획: 개인정보 침해에 대비하여 누가 책임자이며 누가 누구에게 정보를 제공하여야 하는지 그리고 어떤 경우에 보고가능한 개인정보 침해에 해당하는지에 대한 규정을 포함하는 적절한 보고 절차를 수립한다.
- 이에 따라 직원을 교육한다.
- 대비 상태를 유지하기 위해 계획 및 메커니즘이 정상적으로 작동하는지를 점검한다.
- 보고해야 하는 경우에 대비하여, 관할 감독기구의 연락처를 숙지한다.

12 GDPR 준수를 입증하는 방법

개인정보 감독기구는 IT 부문 기업에서 일반적으로 이용 가능한 인증을 GDPR의 준수에 대한 충분한 증거로 인정하기를 다소 꺼린다.

그러나 점점 더 많은 기업이 법적 요건을 준수하고 있음을 표준과 인증을 통해 입증하고자 한다. GDPR을 입법한 의원은 이런 전개 과정이 GDPR 제40조와 제42조 제(1)항에 명시된 바와 같다고 인정하였다. 따라서 컨트롤러와 프로세서는 GDPR을 “준수하고 있음을 입증하기 위해” 이러한 행동 규약과 인증 제도를 수립해야 한다.

인증 받는 것은 그 자체로 GDPR에 대한 준수를 증명하는 것이 아니라, 오히려 준수에 대한 입증 방법 중 하나이다. 그러나 GDPR에서 알 수 있듯이 GDPR 인증서를 발행하도록 승인된 행동 규약, 인증 제도 또는 공인 인증기관은 현재까지 없다.

물론 GDPR이나 최소한 그 일부의 준수에 대한 증거로 EU 내 규제기구가 보증하는 일부 표준과 모범사례가 있다. ISO 27001에 따른 인증은 최소한 GDPR 제32조가 규정하는 준수 요건의 일부를 인증하는 것에 대해 널리 알려진 접근법이다. 또한 GDPR 제40조에 따른 GDPR 인증 제도는 아직 발표되지 않은 반면, 많은 GDPR 및 IT 보안 관련 제도가 실무에서 정기적으로 사용되고 있다.

규제기구가 보증하는 GDPR 인증에 대한 정보를 수집하기 위하여 현재의 전개 상황을 면밀하게 모니터링 한다.

V 진출 기업의 업무 유형별 대응사례 제시

아래에서는 GDPR 준수를 위해 조치하고 있는 대표적인 실제 사례를 제시한다. 기업의 규모 및 관련 산업과는 상관없이 아래 시나리오 중에서 최소한 한 개 또는 두 개의 시나리오를 검토하는 것을 권장한다.

1 웹사이트 및 앱을 운영하는 경우

거의 모든 기업이 웹사이트, 소셜 미디어 페이지 또는 앱을 운영하므로 GDPR의 적용 대상이다. 최소한 EU 역내에 있는 자연인을 대상으로 운영하는 경우, GDPR의 적용 대상이 된다(지리적 적용 범위에 대해서는 상기 제2절 참조). 이는 유럽의 구독자를 대상으로 하는 웹사이트를 운영하는 경우(현지 언어의 지원 여부는 상관없이), GDPR을 적용하는 것을 의미한다. 추적 정보(예: 추적 쿠키나 리타겟팅/광고 네트워크)를 사용하여 유럽 웹사이트 사용자를 목표로 하거나 IP 주소 또는 기타 개인 식별자와(예: 장치의 MAC 주소 등) 같은 로그 파일을 수집하는 경우, GDPR이 적용될 수 있다는 사실을 유념한다.

고객과 소통하는 주요 플랫폼으로 웹사이트, 소셜 미디어 페이지 또는 앱을 운영하는 경우, GDPR의 전체적인 준수 여부에 엄청난 영향을 미친다.

첫 번째 단계로 필수적인 것은, 체계적인 개인정보 처리방침을 수립하는 것이다. 광범위한 통지 의무(3.1 참조)를 충족하기 위해 웹사이트/앱을 검토 및 평가해야 개인정보 보호와 관련한 기능을 결정할 수 있다. 이러한 평가와 결정을 통해 귀사는 사용자에게 적합한 정보를 제공할 수 있다.

적합한 개인정보 처리방침을 수립하는 것뿐만 아니라 개인정보 수집 및 처리 방식이 적법한지도 평가해야 한다. 웹사이트에 적용하는 가장 일반적인 기능은 다음을 포함한다.

1. 추적 도구(예: Google analytics)
2. 등록 서식
3. 뉴스레터 가입 서식
4. 쿠키
5. 소셜 미디어 버튼
6. 연락처 서식
7. 전자 상거래 사이트 상의 지불 게이트웨이(예: Paypal)

각 처리 활동에 대해 법적 근거가 있어야 한다는 점에 유의한다. 웹사이트를 제공하는 경우, 일반적으로 „계약 이행“(GDPR 제6조 제(1)항 제(b)호, 예: 이메일 문의에 대한 응답)이나 “적법한 이익“(GDPR 제6조 제(1)항 제(f)호, 예: 기술적 보호조치 적용 또는 일부 마케팅 활동 실시)로 좁혀진다.

■ 주의 사항

웹사이트와 앱의 사용을 평가하기 위해 사용 프로파일(추적)을 생성하는 경우, 개인정보 처리방침에 대한 보고서를 통해 항상 정보주체에게 이에 대해 통지해야 한다.

국가 법률이 허용하거나 정보주체가 동의한 경우에만 개인 추적을 실시할 수 있다. 최근 유럽의 규제기관은 이런 과정에 대해 매우 엄격하며, 많은 활동에 대한 동의를 요구한다. 절차가 전체적으로 적법하더라도 추적 및 마케팅 활동에서 쉽고 분명하게 탈퇴할 수 있는 기회를 정보주체에게 항상 제공해야 한다.

웹사이트나 앱이 등록 사용자만 열람 가능한 장소에 있는 개인정보에 접근할 수 있는 경우, 정보주체를 식별 및 인증하여 개인정보를 충분히 보호해야 한다.

또한 웹사이트의 보안을 강화할 것을 고려한다. 처리한 개인정보를 충분히 보호하기 위한 조치를 취해야 한다. 보안 조치는 다음을 포함한다.

- 암호화
- 안전한 호스트의 사용(호스팅 회사의 보안 계획과 보안 수준 확인)
- 웹사이트의 지속적인 유지 보수 및 소프트웨어의 최신 상태 유지
- 엄격한 접근 제어 및 비밀번호 정책
- 신뢰할 수 있는 백업 루틴(backup routine) 수립
- 정기적으로 보안 확인

웹사이트는 GDPR준수를 위한 몇몇 수단을 취해야 한다. 그러나 우선 다음 사항을 철저히 게 확인하고 가장 관련이 있는 요건을 요약하여야 한다.

■ 체크리스트

- 웹사이트, 앱 또는 웹서비스에 있는 개인정보 보호 관련 기능을 확인한다.
- 각 목적이나 기능에 대해 적절한 법적 근거를 마련한다.
- 모든 목적과 기능이 필요한지, 또는 개인정보 보호에 보다 친화적인 대안을 사용하여 그러한 목적과 기능을 대체할 수 있는지 여부를 검토한다.
- 개인정보 보호의 관점에서 유럽 역내에서 추적과 온라인 마케팅을 실시하는 것은 매우 복잡한 작업이다. 이는 현재 과도기에 있다. 사용하고자 하는 도구나 절차와 관련하여 동의를 별도로 받아야 하는지 여부 및 동의 받는 방법을 검토한다.
- 이에 따라 개인정보 처리방침 초안을 작성하거나 수정한다. 이는 GDPR 웹사이트 개념에 있어 핵심적인 부분이다. 항상 더 많은 정보를 제공할 것을 권고한다.
- 보안 계획을 점검하고 이에 따라 행동한다!

2 현지 직원의 개인정보 처리절차

소규모 기업일지라도 구직자, 직원 또는 노동자의 개인정보를 수집 및 사용할 것이다. 직원이 유럽 역내에 있는 경우(예: 그룹에 속하는 기업 중 하나가 유럽 역내에 있는 경우), 직원의 개인정보를 처리하는 데 있어 GDPR의 요건을 준수해야 한다. 이 안내서에서 규정한 모든 규칙을 예외 없이 적용한다. 또한 직원의 개인정보 처리 시 매우 일반적으로 수행하는 일부 처리 활동은 추가 단계를 요구할 수 있다.

요약하면 고용주는 고용 관계의 시작 단계부터 고용 도중 및 종료 이후에도 직원의 개인정보를 보호해야 한다.

■ 예시

- 시작 단계: 직원 채용 시 입사 지원서와 이력서를 통해 개인정보를 요구하고 수령함으로써 직원의 개인정보를 수집한다.
 - 고용 도중: 급여 및 혜택에 대한 자격, 인사 고과, 징계 및 불만 사항과 관련한 개인정보를 처리한다.
 - 종료 이후: 일정 기간 동안 개인정보(예: 세금 규정, 법정 병가 급여 등)를 보유해야 하는 법적 의무가 있다.
- 유의 사항: 직원의 개인정보를 처리하는 경우, 적법한 근거가 있어야 하며 제한된 기간 동안 공정하게 처리하고 정확하고 안전하게 보관할 것을 보장해야 한다.

직원을 고용하는 도중 이와 관련된 정보처리 활동을 추가적으로 실시할 수 있다. 회사 IT 시스템(예: 시스템 로그 파일)의 무결성을 보장해야 하는 보안 목적을 위해 직원의 개인정보를 수집할 수 있다. 사업장 내에 CCTV를 설치하는 경우, 카메라는 직원을 기록할 것이다. 이 경우에 법적 요건을 철저히 평가해야 한다. 또한 병가를 관리하는 경우, 민감정보(예: 건강에 대한 개인정보)를 수집하고 처리할 수 있으며 특별한 주의를 기울여 이러한 민감정보를 취급해야 한다.

동의를 자유의사에 따라 받아야 하며, 고용 관계에서는 동의의 유효성에 대하여 종종 의심을 받기 때문에 직원의 동의에 기초하여 처리 활동을 수행하기가 매우 어려울 것이다. 따라서 동의를 적절한 근거로 사용하여 개인정보를 처리하는 경우에는 주의해야 한다. 대부분의 경우 동의는 실질적인 법적 근거가 될 수 없기 때문이다.

어떤 경우에도 **직원 개인정보 처리방침**을 수립하는 것이 매우 중요하다. 이러한 취급방침은 관련 법률을 준수하지 않는 데 대한 불만이 제기될 위험을 크게 줄일 수 있다. 이 취급방침은 관련 처리 목적, 수집한 개인정보, 개인정보 처리자, 직원이 추가 정보를 구할 수 있는 방법 및 정보주체로서 자신의 권리를 행사할 수 있는 방법을 모두 나열해야 한다. 종종 적법한 이익에 기초하여 직원의 개인 정보를 처리할 수 있기 때문에 정보주체에게 적절하게 정보를 제공하는 것이 더욱 중요해질 것이다.

직원의 개인정보 보호는 매우 복잡한 주제이기 때문에 이에 대해 보다 상세하게 설명할 수도 있다. 그러나 개인정보 처리에 대한 다음 원칙은 훌륭한 체크리스트를 제공할 것이다.

■ 체크리스트

- ☑ 직원도 GDPR에 따른 정보주체라는 사실을 유념한다!
- ☑ 직원의 개인정보를 처리하는 경우나 직원(위치에 상관없이)에 대한 처리 활동이 유럽 역내에 기초하는 경우, 앞에서 설명한 GDPR 규칙이 직원에게도 적용된다.
- ☑ 모든 처리 활동에 대하여 법적 근거가 있는지를 점검한다. 동의에 기초하여 처리 활동을 수행하는 경우, 자유의지에 따라 동의를 제공하도록 보장한다. 그러나 다른 법적 근거를 찾을 수 있는지 확인한다.
- ☑ 직원 개인정보 처리방침을 수립한다! 이는 직원 개인정보의 용도를 파악하고 지침을 제공하며 직원 개인정보 처리 방향을 결정하는 데 도움이 된다. 건전한 직원 개인정보 보호 정책은 직원의 개인정보를 보호하는 데 있어 확실한 근거가 될 것이다.
- ☑ 여러 EU 회원국이 자국의 개인정보 보호 법률에서 직원 개인정보 보호에서 벗어나는 규칙을 규정한다는 점을 고려한다. GDPR은 이러한 여지를 남기고 있다. 이는 임직원이 전 유럽을 아우르는 개인정보 보호 법률 개념을 설계하는 것을 매우 어렵게 한다. 처리 활동이 어디서 일어나는지에 따라 상황이 달라질 수 있다는 점을 인지해야 한다. 따라서 필요한 경우, 다시 확인한다!

3 마케팅을 수행하는 경우

마케팅과 GDPR은 서로 조화를 이루기가 매우 어려울 수 있다. 마케팅은 사업이나 조직을 운영하는 데 있어 필수적인 부분이다. 현재 보유한 정보에 기초하여 기존 및 잠재 고객의 요구와 원하는 바를 파악하거나 예측하는 것은 마케팅의 고유한 특성이다. 이를 위해서는 개인정보가 매우 중요하다. 다른 한편, GDPR은 회사가 고객과 소통하는 방식을 변경하였다. 대중의 인식이 개선됨에 따라 고객은 불만사항 발생 시, 더 이상 참지 않고 감독기구에 민원을 제기한다. 따라서 마케팅을 위해 고객의 개인정보를 사용하는 경우에는 더욱 주의해야 한다.

마케팅과 그에 적용 가능한 법체계를 검토하는 경우, EU 역내에는 이러한 활동을 규제하는 법률이 여러 개 있다는 것을 고려한다. GDPR뿐 아니라 일부 국가의 법률이 전자적 수단(예: 이메일 등)을 통한 마케팅 활동을 규제한다. 이와 동시에 유럽의 여러 의원은 특히 온라인 및 미디어 개인정보를 포함하는 새로운 “전자프라이버시 규정(ePrivacy Regulation)”에 대해 논의한다. 원래 “전자프라이버시 규정(ePrivacy Regulation)”은 GDPR과 함께 발효될 예정이었으나 여전히 계류 중이다.

그러나 EU 회원국의 특정 법률(예: 독일의 불공정 경쟁에 대한 법(Law against Unfair Competition))에 따르면, 뉴스레터 발송, 이메일을 통한 제안, 전화를 통한 정보 제공과 같은 마케팅 목적을 위해서는 정보주체의 명시적 동의가 필요하다. 이에 대해서는 다소 엄격한 공식 요건을 준수해야 하며, 예외를 매우 제한적으로 적용한다.

GDPR은 개인정보에 대한 마케팅 목적의 사용을 컨트롤러의 적법한 이익으로 인정한다. 그러나 GDPR에 따르면 동의가 없는 경우에는 이러한 활동이 제한된다. 특정 유형의 고객 프로파일링, 웹 추적 및 민감정보를 사용하는 경우 별도의 동의가 필요할 수 있다.

어떤 경우에도 고객이 마케팅 정보 수신에 대한 동의를 철회하면 이를 엄격하게 준수하여야 한다. 고객이 원하지 않을 경우, 기업은 직접 마케팅 활동을 수행해서는 안 된다.

이메일을 통한 마케팅의 경우 책임성의 원칙을 따르는 데 있어 입증 가능한 동의를 구하기 위하여 **더블 옵트인(double opt-in)** 절차를 권고한다. 이는 광고주가 동의를 제공한(예: 웹사이트를 통해 등록) 고객이나 파트너에게 이메일을 보내고 해당 동의에 대해 확인하도록 요청하는 것을 의미한다. 이러한 확인을 받은 경우에만 마케팅 정보를 보내야 한다. 또한 이에 관해 항상 적절하게 문서화하고 보관해야 한다. 동의를 제공한 경우, 마케팅을 위해 고객이나 파트너와 접촉할 수 있다. 수령인이 반대한(소위 “옵트아웃(opt-out)”) 경우는 제외한다.

위에서 설명한 바와 같이 이 분야에서는 고객과의 분쟁이 정기적으로 발생하기 때문에 모든 고객의 요청을 진지하게 고려하고 이에 즉시 대응할 것을 권고한다. 다음 체크리스트는 이런 개념을 적절하게 구현하는 데 도움이 될 수 있다.

■ 체크리스트

- 모든 마케팅 활동을 조사하고 동의를 받았는지 또는 필요한 경우 다른 법적 근거가 있는지를 검토한다.
- 필요한 경우, “적절한 방법”으로 동의를 받을 것을 보장한다(예: 옵트인, 사전에 선택되어 있지 않은 체크박스 등).
- 마케팅과 관련한 개인정보를 사용하는 방법에 대해 정보주체에게 정보를 제공한다(예: 개인정보 처리방침).
- 특정한 처리 활동이 추가적인 개인정보보호 절차를 요구할 수 있다는 것을 고려한다(예: 프로파일링이나 타겟팅과 관련한 경우).
- 신뢰할 수 있는 대응 계획을 수립하고 고객의 요청에 즉시 대응한다! 그렇지 않을 경우, 고객이 감독기구에 민원을 제기할 수 있다.

4 빅데이터를 활용하는 경우

빅 데이터는 사업을 더 잘 이해하고 사용 가능한 개인정보로부터 흥미로운 결론을 내리기 위하여 방대한 양의 개인정보를 사용하는 방법이다. GDPR로 인한 제약 사항 때문에 빅 데이터에도 몇 가지 어려움이 있다.

첫째, 빅 데이터를 활용하는 경우, 이를 위해 사용하는 거의 모든 정보는 개인정보라고 가정한다. 분석에 사용하는 개인정보의 양이 클수록 특정 개인정보를 연결함으로써 자연인을 재식별할 가능성이 커진다. 따라서 빅 데이터를 활용하는 경우, 가장 중요한 목표는 익명처리한 개인정보를 사용하는 것이다. 이런 목적을 달성하는 방법을 더 잘 이해하기 위해서는 상기 2.1절을 참조한다. 빅 데이터를 위하여 데이터셋을 적절하게 익명처리하는 것은 매우 어려운 과제이다. 이를 달성할 수 있는지에 대해 확신이 없는 경우, GDPR을 준수한다!

고려해야 하는 개인정보 처리 원칙은 평소와 동일하다. 이 안내서의 상기 내용을 참조한다. 빅 데이터 및 GDPR과 관련하여 흔히 나타나는 세 가지의 대표적인 사안을 살펴보자. 첫째, 정보 주체의 개인정보를 취급하는 방법과 관련한 정보를 정보 주체에 제공하여야 한다는 점을 유념한다(GDPR 제13조 및 제14조, 상기 참조). 하지만 일반적으로 기업은 개인정보를 수집한 후에 빅 데이터와 관련하여 개인정보를 사용할 것을 결정한다. 이는 처리 목적의 변경을 의미한다(GDPR 제6조 제(4)항). 이 경우, 법률에 따라 계획에 대한 정보를 투명한 방식으로 정보주체에 제공해야 한다. 이는 정보주체와 함께 이에 대해 논의할 것을 요구할 수 있다(예: 개인정보 보호 정책에 대한 수정안).

둘째, 위에서 설명한 바와 같이 빅 데이터를 위해 개인정보를 사용하는 경우, 일반적으로 처리 목적을 변경하게 된다(GDPR 제6조 제(4)항 참조). 이런 특정한 목적에 대해 다른 법적 근거를 결정해야 한다. 가끔은 적법한 이익에 기초하여 개인정보를 처리할 수 있다(GDPR 제6조 제(1)항 제(f)호). 실제 상황(예: 개인정보 사용 방법, 정보주체를 재식별하는

위험의 정도, 개인정보의 범주 및 중요도 등)에 따라 빅 데이터는 다른 수단이 적법할 것을 요구할 수 있다(예, 정보주체의 별도 동의).

셋째, 개인정보를 열람할 수 있는 개인정보 프로세서(예: 서비스 제공회사)가 빅 데이터 프로젝트에 종종 참여한다. 프로세서가 참여하기 위해서는 GDPR 제28조에 따라 개인정보 처리 계약과 그의 다른 보호조치가 필요하다. 따라서 서비스 제공업체가 개인정보를 열람하는 것을 허가하기 전에 이에 주의해야 한다는 것을 유념해야 한다.

요약하면, 개인정보 수집 및 처리 전에 목표를 정의하는 것이 매우 중요하다. 개인정보 보호 적용 설계(Privacy by Design)는 적절한 단계를 적절한 때에 구현하기 위해 고려해야 하는 주요 개념이다.

5 사물 인터넷(Internet of Things)을 활용하는 경우

사물 인터넷(Internet of Things, IoT)은 GDPR과 함께 중요한 영향을 미치는 다른 방식이다. IoT 서비스를 특징으로 하는 포괄적인 연결과 개인정보 전송을 허용하는 장치를 판매하거나 서비스를 제공하는 경우, IoT 서비스는 항상 개인정보의 수집과 처리를 포함한다.

첫째, 개인정보나 익명처리된 개인정보를 다루는지를 이해하는 것이 중요하다. 예를 들어 스마트 홈 환경에 연결된 장치를 고객이 제어하는 것을 돕는 서비스를 제공하는 경우, 수집한 개인정보는 일반적으로 장치 소유자나 속성에 대한 참조를 포함한다. 이는 고객 ID, IP 주소 또는 다른 식별자를 포함할 수 있다. 익명처리는 실제로 상당히 어려운 일이다.

항상 그렇듯이, IoT 서비스나 장치를 통해 수집한 개인정보를 처리하기 위해서는 법적 근거가 있어야 한다. 계약 이행과 관련한 경우, GDPR 제6조 제(1)항 제(b)호를 귀사에게 유리하게 적용할 수 있다. 하지만 제품 개발, 예측 유지 보수 서비스 또는 판매 및 마케팅 활동과 같은 다른 목적을 위해 수집한 개인정보 사용을 종종 결정할 수 있다. 이러한 목적의

경우, 적법한 이익(GDPR 제6조 제(1)항 제(f)호)이 도움이 될 수 있지만 다른 경우에는 도움이 될 수 없다. 이런 맥락에서 민감정보를 처리하는 경우, IoT 장치와 서비스가 정보주체에 대하여 일부 위험(프로파일링, 자동화된 의사결정 또는 다른 중요정보 처리 활동에서 기인할 수 있는)을 발생시킬 수 있다는 것을 고려한다. 적법한 이익에 기초하여 처리하는 경우, 이는 균형 시험에 큰 영향을 미칠 것이다. 즉, IoT 장치와 서비스에서 발생하는 개인정보를 사용하는 경우, 각 목적에 대해 적절한 법적 근거를 찾아야 한다.

개인정보처리에 대해 동의를 받아야 한다고 결론을 내리는 경우, 다른 장애물을 직면할 수 있다. 개인정보의 처리에 대한 귀사의 역할(컨트롤러나 프로세서)이나 귀사와 정보주체의 관계(정보주체가 귀사의 고객인가 아니면 다른 회사의 고객인가?)에 따라 동의를 받는 것이 어려울 수도 있다. GDPR 제13조와 제14조에 따라 정보주체에게 정보를 제공해야 하는 경우, 같은 장애물을 직면할 수 있다.

특히 정보주체와 귀사와 직접 관계가 없는 경우, 이는 특히 다루기 어려운 문제일 수도 있다. 이는 귀사가 IoT를 앱이나 웹서비스와 함께 운영하지 않는 경우, IoT 장치가 개인정보 보호 법률과 관련한 정보를 표시하는 적절한 메커니즘을 제공하지 않기 때문이다. 마지막으로, IoT 장치와 서비스는 방대한 양의 개인정보를 수집하는 경향이 있기 때문에 이를 추후에 제거하는 것은 항상 어려운 과제이다. 따라서 이런 맥락에서 개인정보를 수집하는 경우, 개인정보 처리의 최소화 원칙을 늘 고려하고, 개인정보를 적절하게 보유하고 추후에 과기하는 방법을 생각해야 한다.

6 의료 서비스를 제공하는 경우

앞에서 이미 설명한 바와 같이, 민감정보를 처리하는 경우, 특히 개인의 건강과 관련이 있는 경우, GDPR은 보다 주의할 것을 요구한다. GDPR은 “유전” 및 “생체 측정” 개인정보를 사용하는 것을 규제한다. 따라서 GDPR이 건강 부문에서 개인정보의 처리를 분명하게 규

제하고 다른 종류의 개인정보를 다루는 경우보다 더 엄격한 요건을 컨트롤러(와 프로세서)에 부과한다는 것을 알 수 있다.

원칙적으로는, 정보주체가 명시적으로 동의하는 경우에만 개인의 건강정보를 처리할 수 있다. 해결책 중 하나는 개인정보를 처리하기 전에 개인정보를 익명처리하는 것이다. 이는 매우 제한적인 경우에만 효과가 있다. 그러나 달성할 수 있는 경우, 이는 모범사례가 될 것이다. 비록 규제기관이 익명처리와 관련하여 구체적인 지침과 표준을 아직 제공하지 않았지만, 개인 건강 정보의 처리와 관련한 위험이 매우 높기 때문에 그 기준을 높이 설정하는 것은 공정한 것이다.

이는 개인 건강 정보를 처리하는 데 항상 동의를 구해야 한다는 것을 의미하지는 않는다. GDPR은 예를 들어 병원을 운영할 때 계약상 의무(건강 관련 서비스의 전달 등)를 이행하기 위해 개인 건강 정보가 필요하다는 것에 사실에 기초하여 개인 건강 정보 처리를 허용한다. 그러나 계약을 이행하기 위해 필요한 것을 법률이 정의하는 정도에 따라 엄격하게 해석한다(GDPR 제9조 제(2)조 및 이와 관련한 국가의 법률 참조. 예를 들어 임직원 개인 정보 보호 부문에서).

예를 들어 사용자의 건강 개인정보를 사용하여 생성한 프로파일을 원래 개인정보를 요청한 목적(환자의 치료 등)과 다른 목적을 위해 사용하는 경우, 일부 처리 활동은 이러한 범위에 해당하지 않을 수 있다. 이 경우에는 동의를 받아야 할 필요가 있다.

개인의 건강 정보를 제3자(예: 기술 서비스 제공업체)에게 이전하는 경우, 일반적으로 매우 엄격한 보호조치가 필요하다. 처리 활동의 중요도와 GDPR의 일반 규칙(GDPR 제9조 참조)을 고려하여 동의를 받을 것을 권고할 수 있다. 그러나 최근에 이러한 종류의 서비스에 대한 일부 예외가 발표되었다. 따라서 전송 및 처리를 위해 제3자의 동의를 필요하지 않을 수도 있다.

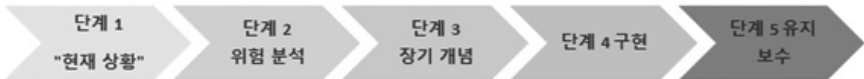
그러나 여러 EU 회원국은 GDPR과 함께 적용하는 형법에 따라 환자의 개인정보 공개를 엄격하게 규제하기 때문에 개인정보 처리 활동을 철저히 평가할 것을 적극적으로 권고한다. 이러한 종류의 서비스를 제공하는 경우, 엄격한 기술적·관리적 조치(GDPR 제32조)가 GDPR을 준수하는 데 있어 주요 구성요소이다.

또한 개인정보 보호 적용 설계와 개인정보 보호 기본 설정에 초점을 맞추어야 한다. 이 요건은 개발 단계에 있는 회사가 가능한 한 적은 개인정보를 수집하는 방식으로 서비스를 구조화하고 개발할 것을 요구하기 때문이다.

VI 단계별 가이드(Step-by-Step Guide)

본 안내서에 포함된 조항과 정보의 양이 방대하다는 점을 감안할 때, 기업이 GDPR를 준수하도록 하는 것이 매우 어려운 일처럼 보일 수 있다. 그러나 가장 중요한 것은 시작하고 조치를 취하는 것이다.

다음 접근법을 권고한다.



모든 단계를 문서화한다. 책임성!

단계 1: 제공한 체크리스트를 사용하여 현재 상황을 분석한다

- 프로젝트를 포함하도록 자원과 예산을 할당한다(오랜 시간이 걸릴 수 있다).
- GDPR 핵심 부서(core team)를 지정하고 각 부서에서 한 명의 책임자를 지명한다.
- 경영진이 주목하도록 한다. GDPR이 초래하는 위험은 인식을 개선하는 데 충분할 것이다.
- 다음을 명확하게 한다.

- 어떤 종류의 개인정보를 처리하는가?
- 어떤 종류의 처리 활동을 하는가?
- 어떤 목적을 위하여 개인정보를 처리하는가?
- 어디에, 어떻게, 그리고 얼마나 오랫동안 개인정보를 보유하는가?
- 누가 개인정보를 열람하는가?
- 법적 근거는 무엇인가?

단계 2: 잠재적 위험을 분석한다

- 모든 부서의 감사 결과를 분석하고, 특히 가장 큰 위험과 관련한 절차에 대하여 분석한다.
- 이에 따라 우선순위 목록을 정한다.
- 가장 위험한 우려 사항을 먼저 다룬다.
- 첫 번째 구제 제도를 적용한다(예: 개인정보 처리방침, 개인정보 처리 계약, 동의서 등).

단계 3: 장기적 개념을 개발한다

- 향후에 발생할 수 있는 상황을 먼저 파악한 후에 자원과 예산을 할당한다.
- GDPR 보호조치를 구현하고 절차를 감독할 책임자(내부 인력이나 외부 고문)를 지정한다.
- GDPR를 기회로 여긴다(개인정보의 양을 간소화하고 프로세스의 효율성을 개선하며, 오래된 시스템을 삭제하고 새롭고 더 효과적이며 안전한 기술로 업그레이드한다).

단계 4: 구현한다

- 필요한 조치를 단계별로 구현한다.
- 중요한 절차와 덜 중요한 절차 사이에 우선순위를 정한다.
- 가동 준비를 한다 - 협력하여 행동한다.
- 워크숍과 교육을 통해 인식을 개선한다.

단계 5: 유지 보수한다

- 메커니즘이 신뢰할 수 있게 작동하도록 계속 점검한다.
- 필요한 경우, 절차를 조정한다.
- 새로운 기술 발전, EU 및 국가의 법률과 감독기구의 결정(즉 벌칙의 집행)에 주목한다.

VII GDPR에 대한 추가 정보 및 관련 출처

본 안내서는 GDPR 중 가장 관련 있는 측면에 대한 제한적인 개요만 제공하기 때문에, 본 지침을 모두 읽은 후 GDPR에 대한 더 상세한 지침과 자료를 원할 수도 있다.

GDPR의 해석 및 적용에 대한 지침을 발간하는 EU 개인정보 보호 위원회(European Data Protection Board(前 제29조 작업반))의 웹사이트(*)를 참고할 것을 권고한다. 이러한 지침은 법적 체계를 더 잘 이해하는 데 도움이 되며 GDPR을 일상 업무에 적용하는 방법에 대한 여러 예시를 제공한다.

(*)edpb.europa.eu/edpb_en

EU 개인정보 보호 위원회의 내용을 검토하고 GDPR을 보다 철저히 준수하는 데 큰 도움이 되는 조사 보고서를 다운로드 할 수 있다.

| | |
|--|---|
| GDPR (제3조)의 지리적 적용 범위에 대한 2018년 3월 지침 | https://edpb.europa.eu/sites/edpb/files/consultation/edpb_guidelines_3_2018_territorial_scope_en.pdf |
| 동의에 대한 지침(WP259rev.01) | https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=62305 |
| 투명성에 대한 지침(WP260rev.01) | https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=622227 |
| 자동화된 개별 의사결정 및 프로파일링에 대한 지침(WP251rev.01) | https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612053 |
| 개인정보 침해 통지에 대한 지침(WP250rev.01) | https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612052 |
| 데이터 이동권에 대한 지침(WP242rev.01) | https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611233 |

| | |
|---|---|
| 데이터 보호 영향평가(DPIA) 및 데이터 처리가 “고위험을 초래할 가능성이 있는지”를 결정하는 데 대한 지침(WP248rev.01) | https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611236 |
| 개인정보보호 책임자(DPO)에 대한 지침 (WP243rev.01) | https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612048 |
| 컨트롤러 또는 프로세서의 주요 감독당국을 식별하는 것에 대한 지침(WP244rev.01) | https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611235 |
| GDPR 제30조제(5)항에 따른 처리 활동에 대한 기록 유지 의무 수정에 대한 성명서 | https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=624045 |
| GDPR에 따른 컨트롤러 및 프로세서에 대한 “구속력이 있는 기업 규칙”의 승인을 위한 협력 절차를 규정하는 작업 문서(WP263rev.01) | https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=623056 |
| 개인정보 이전을 위해 컨트롤러에게 구속력이 있는 기업 규칙 승인을 위한 표준 신청에 대한 권고 사항 (WP264) | https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=623850 |
| 적절성 참고문서(WP254rev.01) | https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=614108 |
| 과징금의 적용 및 설정에 대한 지침(WP253) | https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611237 |

상기 목록은 현재 사용 가능한 지침의 일부를 발췌한 것이다. 추가 문서에 대해서는 웹사이트를 참조한다.

또한 역외 개인정보 이전에 대한 현재 샘플 문서를 포함하여 EU 표준 개인정보보호 조항에 기초한 역외 개인정보 이전에 대한 지침이 EU 집행위원회의 웹사이트^(*)에 게재되어 있다. 아울러, 프랑스, 독일 등은 EU국들은 국별 개인정보 보호기구를 통하여 GDPR 준수를 위한 기업의 조치사항을 안내하고 있으며, 동 웹사이트에서는 개인정보 처리 계약을 작성하는 방법 등 안전별로 잘 정리하고 있다.^(**)

마지막으로, 독일에 있는 BITKOM e.V. ^(***)와 같은 여러 이익 단체도 도움이 되는 지침을 무료로 인터넷에 제공한다.

(*) ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/model-contracts-transfer-personal-data-third-countries_en

(**) edpb.europa.eu/about-edpb/board/members_en / (France) www.cnil.fr / (Germany) datenschutz-wiki.de/Aufsichtsbeh%C3%B6rden_und_Landesdatenschutzbeauftragte

(***) bitkom.org/E



EU 진출 기업을 위한 유럽 일반 개인정보 보호규정(GDPR) 핸드북

English



British Airways has suffered the biggest fine yet levied under the EU's General Data Protection Regulation (GDPR). The UK Information Commissioner's Office says it intends to fine BA £183m (€204m, \$229m) – 1.5 percent of BA's worldwide turnover in 2017 – after it admitted that more than half a million customers' data had been stolen by hackers last August from its website and mobile app. In the first nine months of GDPR, national data protection agencies in 11 countries had levied a total of €56m in fines, made up mostly of a €50m fine that France's CNIL imposed on Google in January. BA will be able to make representations to the ICO over the finding and fine. (Financial Times, July 9, 2019)

A Handbook to guide companies through the new European Data Protection Framework

GDPR stands for the EU General Data Protection Regulation. The GDPR is the current European wide applicable data protection framework which has entered into force on 25 May 2018. Already before the effective date and ever since, many Korean enterprises within but also outside of the EU were, and still are, confronted with GDPR in their day-to-day business.

But you as many other Korean companies might still ask yourself: What is all this fuss about? What is the GDPR exactly? And why does a European Regulation concern us as a Korean enterprise?

It all comes down to the very broad scope of the GDPR. Firstly, the GDPR lays down rules to the comprehensive protection of natural persons with regard to the processing of personal data, a term which is defined very broadly under European laws. Secondly, the GDPR rules apply to almost all private and public sectors' processing by organisations in the EU but also by organisations outside the EU which target EU residents.

At the heart of the GDPR lies the concept of accountability: organisations need to be able to demonstrate that they have analysed the GDPR's requirements with regards to their processing activities and that they have implemented a system and mechanisms that allow them to achieve compliance - and that they can proof so at any time!

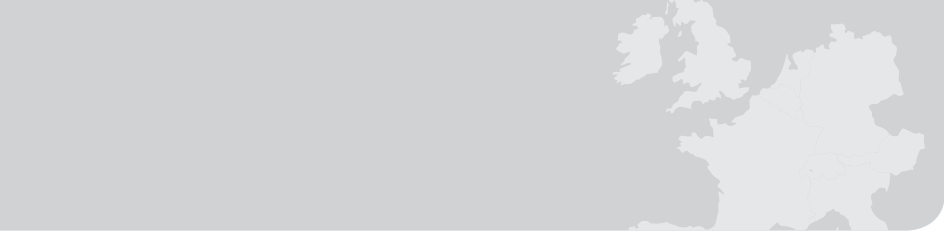
To ensure compliance, the EU dramatically increased the maximum penalties for non-compliance up to EUR 20 million, or four (4) percent of the worldwide turnover of the company group, whichever is higher.

These extensive obligations underpinned with such heavy fines and penalties are part of the reason why GDPR was - and still is - such a hot topic.


Therefore it is important not only for every organisation based in the EU, but also every organisation based abroad that does business in the EU to evaluate whether GDPR applies to them and - in most of the cases - take action in a timely manner.

CONTENTS

| | |
|---|-----------|
| I. How to work with this Handbook | 90 |
| 1. How to read it..... | 90 |
| 2. How to approach GDPR | 91 |
| | |
| II. The 12 Golden Rules | 92 |
| | |
| III. GDPR Glossary – What means what? | 94 |
| | |
| IV. GDPR – What does it require? | 98 |
| 1. Scope – Does the GDPR apply to me? | 98 |
| 1.1 Do we process personal data?..... | 99 |
| 1.2 Territorial scope | 103 |
| 1.3 Personal scope – What exactly is my role? | 105 |
| 2. Processing personal data – How do I do it right? | 111 |
| 2.1. When can I process personal data? | 111 |
| 2.2 Processing special categories of personal data – What is special? ... | 121 |
| 3. What other principles do we have to observe when processing personal data? | 123 |
| 3.1 Transparency under the GDPR – What is required? | 124 |
| 3.2 Purpose Limitation and Data Minimization – What’s to be done? | 127 |
| 3.3 Accuracy and Data Subject’s Rights – How do we ensure that? | 129 |
| 3.4 How is the storage of personal data to be limited? | 129 |
| 3.5 Ensuring Integrity and Confidentiality – How do we do that? ... | 130 |
| 3.6 Privacy by Design & Default | 131 |
| 3.7 Privacy Impact Assessment | 132 |
| 4. Rights of the Data Subjects – What are my obligations?..... | 134 |
| 4.1 Right to Access | 135 |
| 4.2 Right to Erasure, Rectification and Restrictio | 136 |
| 4.3 Right to Data Portability | 137 |



| | |
|---|------------|
| 4.4 Right to Object | 138 |
| 5. Accountability and Documentation – What’s required under the GDPR? | 139 |
| 6. Technical and Organisational Measures – What measures do I have to take? | 141 |
| 7. Data Protection Officer – Do we need to appoint one? | 143 |
| 7.1 What is the role of a Data Protection Officer? | 143 |
| 7.2 Are we obliged to designate one? | 144 |
| 8. Transfer of Personal Data to third parties – What do I need to observe when allowing others to access personal data? | 145 |
| 8.1. Transfer of data to group companies – no intra-group privilege | 146 |
| 8.2. Transfer to processor – data processing agreement required | 146 |
| 8.3. Transfer of Personal Data outside the EU/EEA | 147 |
| 9. What are the consequences of non-compliance? | 149 |
| 10. Working with the supervisory authorities | 150 |
| 11. Data Breaches – What happens if a breach occurs? | 152 |
| 12. GDPR Compliance – Can I certify that? | 154 |
| V. Typical Use Cases | 156 |
| 1. GDPR and operating a website or an app | 156 |
| 2. Employee data – is there anything different? | 159 |
| 3. Marketing – what does GDPR permit? | 162 |
| 4. Big Data | 164 |
| 5. Internet of Things | 166 |
| 6. Healthcare services and GDPR | 167 |
| VI. Step-by-Step Guide | 170 |
| VII. Sources for further information and instructions on GDPR | 172 |



I How to work with this Handbook

1 How to read it

The topic of Data Protection itself is not easy and requires you to get familiar with the specific terms and principles of the GDPR,

This handbook is designed to give you a general overview on what GDPR requires from companies to achieve and to sensitize you to the key challenges of the GDPR,

With this we hope to give you a guiding hand when tackling GDPR compliance at your own organisation or at least bring you a step closer to understanding what GDPR is all about,

Please keep in mind that the following Guidelines are only guidelines and recommendations on how to tread personal data under the GDPR, It shall not provide any binding or compelling rules to obey to. You remain free - at all times - to deviate from these Guidelines as national law or other provisions or rules might provide for further (and even stricter) requirements with regards to certain aspects,

Also, the following Guidelines shall provide a first and rather generic overview and cannot substitute proper legal advice under national laws which is always recommended, In any case, as we believe that the Guidelines are a good start to work your business towards a GDPR compliant setup, we strongly encourage to obey to those principles at any time and where in compliance under national laws,

2 How to approach GDPR

When working your way through this handbook you should try to approach GDPR as follows:

1. Figure out if and why the GDPR applies to you.
2. Understand the purpose and the basic principles of the GDPR.
3. Get familiar with the most relevant requirements of the GDPR.
4. Use the checklists provided to get a basic understanding of your situation.

Get to know first aid measures and apply them. Once you have familiarised yourself with the topic and want a more comprehensive approach, follow the Step-by-Step Guide we have prepared in the last chapter. Keep in mind though that there is no one-size-fits-all solution and it strongly depends on the individual case. After you have completed those steps you might be ready to dive deeper into your compliance project and

5. Implement other required and more detailed safeguards to ensure GDPR compliance.
6. Maintain and regularly check the effectiveness of your measures and constantly improve while taking into consideration current developments.

Becoming GDPR compliant is an iterative and ongoing process as the law develops fast. So, be prepared that GDPR compliance is not a one-stop shop procedure but requires constant attention.




II The 12 Golden Rules

If people ask “What are the most important things I need to know about GDPR?” the answer will usually be that it is simply not possible to narrow the GDPR down to a handful of statements and suggestions. However, if you take anything away from this Handbook, make sure it is these 10 things:

1. *The territorial scope of the GDPR is defined very broadly!* Once you process personal data from EU citizens or a person located in the EU, GDPR will most certainly apply to you.
2. *(Almost) everything is personal data!* If you are not sure if something is personal data, it usually is! Anonymous data is very rare.
3. *Every processing of personal data is forbidden, unless it can be legitimised.* So, to make sure you are compliant when processing personal data you either need a specific rule in the law, explicit consent or a specific legitimate interest while the latter is interpreted rather strictly.
4. *Special rules apply to special categories of personal data.* Processing of e.g. health data will trigger additional requirements which are sometimes really hard to handle. So, if you work with these types of data be aware - it can be a complex undertaking you should check very thoroughly!
5. *Accountability - You have to be able to proof everything!* Although it is a new concept it seems to outrank all the others already. Authorities in Europe will pay a lot of attention to it so better get used to it and design your procedures accordingly.

6. *Transparency - The data subjects always need to know what happens with their personal data.*
Extensive information obligations can be a real struggle for everyone under the GDPR. Get familiar with the concepts at an early stage - before it's too late!
7. *Strong rights of the data subject - be aware and be ready!* Companies need to implement mechanisms to ensure the new and very comprehensive data subject rights under the GDPR are met.
8. *Data Breach - specific requirements ask for specific reporting procedures and strategies.* For example, GDPR leaves controllers 72 hours to notify authorities in case of a data breach; a timeline which can be hard to handle if you do not have a reliable process in place. Take care of it before you really need it!
9. *Intragroup transfer - there is no privilege to transfer personal data within company groups.*
Contrary to what many companies believe, transfer between entities of the same company group follow the same rules as the transfer of data to other 3rd parties. Have data processing agreements in place to steer data transfers.
10. *International data transfer - Korea is not (yet) a safe third country in the meaning of the GDPR.*
Specific rules in accordance with Artt. 44 et seq. GDPR have to be observed before sending data abroad, e.g. by executing special agreements based on the so-called Standard Contractual Clauses (SCCs), which many companies tend to forget.
11. *Data Deletion - harvesting of data just because you can is a no go under the GDPR!* Once you do not need or are permitted to use personal data anymore you need to get rid of it. A proper data storage and deletion concept is a key requirement under the GDPR.
12. *GDPR requires a risk based approach!* GDPR cannot be tackled by implementing a few general rules here and there. It is about the protection of personal data of one or more individuals - and, thus, to assess what is needed always requires a thorough look into the concrete situation! That's why mapping your actual data flows is so important. If you do not follow this approach, you will most certainly not reach GDPR compliance.



III GDPR Glossary - What means what?

The provisions of the GDPR are full of technical terms. So in order to comprehend its subject matter, it is important to first take a look at the terminology.

Accountability - GDPR principle that states that the controller shall be responsible for, and be able to demonstrate compliance with the principles relating to (lawful) processing of personal data.

Accuracy - one of the principles relating to processing of personal data, which entails that personal data always have to be accurate and kept up to date where necessary.

Anonymisation - is the destruction of the identifiable data. In contrast to pseudonymisation (where re-identification of the data subject remains possible), by anonymising personal data can usually not be reassigned to the data subject anymore (or at least with disproportionate means or efforts only).

Consent - the freely given, specific, informed and unambiguous indication of the data subject's wishes or a clear affirmative act whereby the data subject accepts the processing.

Data breach - the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data resulting from a breach of security or access rights; in certain cases a data breach must be reported within established periods to the supervisory authority and the data subjects.

Data Controller - the entity that determines the purposes and means for the processing of personal data.



Data Portability - the requirement for controllers to provide the data subject with a copy of his or her data in a format that allows for easy use with another controller.

Data Processor - the entity that processes personal data on behalf of the Data Controller.

Data Processing Agreement - agreement concluded between Data Controller and Data Processor regarding commissioned data processing which must include: subject-matter, duration of the processing, nature and purpose of processing, categories of personal data and data subjects, obligations and rights of Data Controller and Data Processor and other predefined topics; usually a standard agreement.

Data Protection Impact Assessment (“PIA”) - the evaluation of the impact of the envisaged processing operations prior to the start of the actual processing; this is only necessary in high risk situations (e.g. in the case of new technology or a profiling operation with significant consequences for the data subjects).

Data Protection Officer (“DPO”) - the person (internal or external) who supervises compliance with the GDPR and has the necessary knowledge, resources and authority to do so;

Data subject - the individual to whom the personal data relate. (e.g. employee, customer, …)

Encrypted Data - personal data that is protected through technological measures to ensure that the data is only accessible/readable by those with specified access,

GDPR - the abbreviation for “General Data Protection Regulation” which is an EU regulation that must be applied in its entirety across the EU.

Lawfulness - the principle according to which personal data may only be processed if a valid legal ground exists for doing so (e.g. consent of the data subject, execution of an agreement or the pursuit of a legitimate interest of the controller).

Main Establishment - the place within the Union where the main decisions surrounding data processing are made.

Personal data - any information relating to an identified or identifiable natural person, including indirect identification.

Privacy by Design and Default - GDPR principles that call for the inclusion of data protection from the onset of the designing of systems, rather than an addition at a later stage (“by design”) and according to which “by default” the collection and subsequent processing of personal data shall be limited to what is necessary to achieve each specific purpose of the processing (data-protection friendly pre-settings)

Processing - any action with, or operation performed on personal data, whether or not automated.

Profiling - automated processing of personal data for the evaluation of information relating to a person or in order to analyse or predict her behaviour (e.g. performance at work, economic situation, health, location or personal preferences).

Purpose limitation - the principle according to which personal data may only be processed for specified, explicit and legitimate purposes; the personal data must be limited to what is necessary for these purposes (“data minimisation”) and may only be kept for as long as it is necessary for the intended purpose.

Pseudonymisation - the processing of personal data such that it can no longer be attributed to a single data subject without the use of additional data, so long as said additional data stays separate; a method to substitute identifiable data with a reversible, consistent value, (e.g. a hash number).



Records of processing activities - the Data Controller's records that contain specific information about its processing activities (e.g. purposes, data subjects, personal data, recipients and transfers).


Rights of the data subject - the rights that the GDPR provides for data subjects, such as the right to information and access to personal data, rectification and erasure of the data, objection to direct marketing practices, objection to automated decision-making and profiling and portability of the data.

Sanctions - liability for material and immaterial damage and administrative fines up to 20,000,000 EUR or up to 4% of the total worldwide annual turnover of the company group in the preceding financial year, if this figure is higher.

Special categories of personal data - personal data which reveal racial or ethnic origin, political opinions, religious or philosophical beliefs or trade union membership, genetic or biometric data, data concerning health or a person's sex life or sexual orientation; in principle, the processing of these personal data is prohibited. The generic term Sensitive Data is often used to refer to special categories of personal data and other personal data with a higher need for protection, including financial data such as credit card data whose loss could potentially cause a risk to the rights and freedoms of natural persons (e.g. fraud).

Supervisory authority - the national authority that is responsible for monitoring the application of the GDPR.

Transfers - the transmission of personal data to a country outside of the European Economic Area; such transfer is only possible if done in accordance with the provisions of the GDPR (e.g. standard contractual clauses for a transfer to Korea).



IV GDPR – What does it require?

Now, without further ado, let's go into detail and find out what the GDPR exactly requires you to do. Unfortunately, there is no such thing as a master plan you can follow and then be GDPR compliant. Since the GDPR follows a risk-based approach, the specific requirements and obligations depend on the actual way you process personal data and the level of risk of your processing activities with regard to the data subject's rights and freedoms. The size of your company and the industry you are part of are usually relevant. GDPR applies to any business sector and company size alike. Therefore, you have to take a look at every single one of your processing activities, assess the findings and, based on that, implement the necessary measures.

But first, let's take a step back: maybe the GDPR doesn't even apply to you. And if it does - which will most likely be the case - you should at least know why you, as a Korean organisation, are affected by EU legislation and what that entails.

1 Scope – Does the GDPR apply to me?

When you are figuring out whether or not the GDPR applies to you, ask yourself the following two main questions:

- (1) Do we process personal data?
- (2) Are we within the territorial scope of the GDPR?

1.1 Do we process personal data?

According to Article 2 of the GDPR it applies to the processing of personal data wholly or partly by automated means and to the processing other than by automated means of personal data which form part of a filing system or are intended to form part of a filing system.

In short, the GDPR applies to (almost all) all processing activities of personal data.

1.1.1 Processing of Personal Data – What does it mean?

Thus, to find out whether the use of data will be subject to the strict rules of the GDPR it first needs to be determined whether the action qualifies as *‘processing’* of *‘personal data’* in the meaning of the GDPR which is easier said than done.

‘Processing’ and ‘personal data’ is to be interpreted rather broadly and includes various different actions and categories of data.

However, data that is not personal per se, (e.g. an address or technical data relating to a specific device) might be considered personal from the context it is provided in, such as the combination of non-personal data might lead to an identification of a data subject. An IP address (internet protocol address) for example is deemed to be personal data. Although at first sight it does not reveal any information about a natural person, it still allows a device to be traced back to its user under certain circumstances (e.g. when requesting such information from the competent authorities). The same applies to devices such as mobile phones with an ID connected to it (such as the SIM card or the IMEI number) which competent European authorities might deem to be personal data under certain circumstances.

The GDPR sets out to protect personal data *of any natural person* ('data subject'). This means that not only data of individual customers, but also data of employees as well as data of supplier/service provider employees are included - a fact often overlooked. It is important to note that for the application of the GDPR it doesn't matter whether data is processed in a B2B context (e.g. contact data of a business partner's employee) or in a B2C context (e.g. contact data of a personal that has purchased services).

Rule of thumb: When in doubt, it's personal data!

Whenever personal data is processed - be it by collection, destruction, or any other activity involving personal data - the data protection principles set out in the GDPR apply.

■ Key Definitions and Examples

'Personal data'

A person's name and contact information are typical examples of personal data. However, information such as a person's gender, a customer's purchase history or a person's picture are also to be treated as personal data. There are no exceptions in regard to processing of data in a mere b2b relation. This has the effect that e-mail addresses of business contacts are also considered personal data in the meaning of the GDPR, unless they do not include any identifiable data such as names (e.g. e-mail addresses not assigned to individual persons such as an "info@[●]" address).

'Data subjects'

Please bear in mind that not only your customers are considered data subjects, but also, e.g. your business contacts and employees.

'Processing'

Almost every action performed on personal data such as the collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission (also within a company group), dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction is included therein.

1.1.2 Exception from the rule - Anonymised Data and Pseudonymisation

In contrast to personal data, GDPR does not apply to the processing of anonymised data.

But what is anonymised data? And what is pseudonymisation?

To deem data as being anonymised it is necessary that data can no longer be attributed to a specific data subject. Hence making identification of individuals either impossible or requiring inordinate effort. This can be hard to achieve in practice as really all identifiers need to be removed. This is particularly difficult with large data sets (big data) as the combination/aggregation of data, even not evidently personal might make identification possible.

Amongst many more, there are two main techniques to achieve anonymisation: randomisation and generalisation.

- **Randomisation:** any technique that alters the accuracy of data in order to remove or blur the strong link between the data and the individual.

■ Example

- Replacing data values with a constant symbol (e.g. "*" or 'x')
- Deleting a certain number of bits of IP addresses (for example 8 bits from an IPv4)

- **Generalisation:** the attributes of a data subject are diluted.

■ Example

The collection of a region instead of a city or a month rather than a specific date.

Where you deem data **anonymised** GDPR and its strict requirements will **not apply** per se!

In contrast to anonymised data, GDPR **does apply** to pseudonymised data. **Pseudonymisation** means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information (identifier).

■ Examples

Replacing customer information such as names and contact information with reference numbers while only one person or a selected group independent person knows about the assignment rule for the reference numbers.

Please note that pseudonymised data still falls within the scope of the GDPR, since the risk of re-identification is higher than with anonymous data. Nevertheless, pseudonymisation is one way to fulfil your obligations under the GPRR, e.g. privacy by design or data minimization which might help particularly when processing data based on legitimate interests (Art. 6 (1) (f) GDPR; see below for details). So, pseudonymization should always be a measure you should consider where you can.

If you process personal data in the above sense you fall within the so called ‘material scope’ of the GDPR.

1.2 Territorial scope

Now that we have established that you (possibly) process personal data in the meaning of the GDPR, the second - and sometimes even more pressing - question remains: Are we - as a Korean enterprise - affected? Do we fall within the territorial scope of the GDPR?

The territorial application of the GDPR is very broad and goes beyond European borders (see Article 3 GDPR). In principle, the GDPR applies in two cases:

On the one hand, this is always the case when an entity has an establishment within the EU (so called establishment principle). This can potentially apply even if the relevant data processing takes place outside the EU (Art. 3 (1) GDPR). To qualify as an establishment, a stable arrangement of human and material resources is necessary. The establishment within the EU does not necessarily have to actively participate in the processing (e.g. have possession of personal data). However, it would be enough that it somehow supports the processing of another outside European establishment by providing supporting services (e.g. sales or marketing). At least this is the - very strict - view as proclaimed by the European data protection authorities (c.f. EDPB, Guidelines 3/2018 on the territorial scope of the GDPR (Article 3), page 4 et seq.; see Section VI. Below for further details) If you want to be on the safe side you should follow this interpretation.

On the other hand, the GDPR applies if data of a data subject who is located in the EU is processed - even when doing so abroad. The fact that the controlling company is located outside the EU is irrelevant in this respect. Once the objective of a company is targeting the market of the European Union and its customers located there it is very likely to be within the scope of the GDPR. This is the case for example, when an entity outside the EU offers its services and/or products in the EU or if it monitors the behaviour of individuals located

in the EU (e.g. when collecting respective personal data via a website which might include web targeting or alike as well).

As you can see, it is rather easy to fall into the scope of the GDPR as almost everything that is related to Europe will usually trigger GDPR's applicability. If you do,

■ Appointment of a Representative by Non-EU entities

If you fall within the territorial scope of the GDPR and you are not established in the EU, you might have to appoint a representative in the EU pursuant to Art. 27 GDPR. According to Art. 4 No. 17 GDPR a 'representative' is a natural or legal person established in the EU who represents the controller or processor with regard to their respective obligations under the GDPR. This is to ensure that Supervisory Authorities and data subjects have a contact point within the EU.

The obligation applies to controllers and processors alike – what a controller and a processor is, we'll come to in a minute.

The basic requirements are:

- The representative needs to be established in the EU and needs to be designated in writing. As it needs to "represent" a power of attorney is necessary.
- The law provides the possibility to designate one representative for several controllers and / or processors as long as there are no conflicts of interests.
- It needs to be done before starting the processing of personal data under the GDPR.
- Acting as a representative is a task that can be performed by specialized service providers which you may find on the internet or by referral through KOTRA.

There might be exceptions to appoint a representative which usually narrow down to scenarios where personal data is processed on an occasional basis only and where it does not include the processing of sensitive categories such as health data or invasive technologies (e.g. big data; see Art. 27 (2) GDPR).

1.3 Personal scope – What exactly is my role?

Since the GDPR applies to anyone processing or controlling the processing of personal data, regardless of the legal form of the entity, the range of norm addressees is extensive. But in order to know your role and the actual data protection responsibilities arising therefrom, you need to determine first if you are considered a ‘controller’ or a ‘processor’ within the meaning of the GDPR.

1.3.1 Controller – Who is a controller?

According to Article 4 No. 7 GDPR ‘controller’ means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data.

Thus, controllership depends upon decision-making power and not upon the execution of data processing. It can therefore result from express or implied legal responsibility or from actual influence regarding the purposes and means of processing. Another indicator for being a controller usually is that you process personal data for your own business purposes and not those of other companies.

■ Example

Korean enterprise operating a webshop and selling goods to EU customers would be deemed a controller where processing personal data such as customer names, addresses, payment data etc. for own business purposes while determining the means of the processing (e.g. from a technical and organisational perspective). As the processing is related to the selling of goods the processing occurs for own business purposes.

So, to check whether you are considered a controller go through the following steps:

■ **Checklist**

- ☑ Who decides upon the purpose of processing and its essential elements? Is it you or another entity and what is your relation to it?
- ☑ Who chooses which data shall be processed for how long?
- ☑ Who chooses who shall have access and what security measures need to be taken?
- ☑ Is the processing related to serving your own business purposes or are you acting as a service provider to someone and are you, thus, serving the business purposes of others?

The controller is responsible for compliance with the principles governing the processing of personal data under the GDPR and must be able to demonstrate such compliance.

The most relevant principles the controller has to take care of include:

■ **Art. 5 GDPR Principles**

- Legality
- Fairness & transparency
- Data minimization
- Accuracy of the data processed
- (Temporal) storage limitation and integrity
- Confidentiality of personal data

In particular, a controller shall be responsible for implementing appropriate technical and organisational measures to protect personal data, taking into account the nature, extent and



purposes of the processing and the likelihood and seriousness of the risks to the rights and freedoms of natural persons (see Art. 25 and 32 GDPR).

This was just a first look at the principles. We'll look into these in more detail in a minute.

Also, if you as a controller place an order for data processing with other agencies or companies - let's get to details what that really is in a second - you must do so on the basis of a written contract pursuant to Art. 28 GDPR as you have to make sure that the processor complies with certain basic principles. Such a contract has to include several points pre-determined by law (see Art. 28 GDPR).

1.3.2 Joint Controller - Where is the difference?

If several data controllers jointly define purposes and means for data processing, they are 'joint controllers'. Since this is a fairly new mechanism in European law there is uncertainty as to when this will be the case or not. As a rule of thumb, a Joint Controllershship needs to be considered where two or more entities work very close together in a collaborative manner to design and perform certain data processing activities. This can also be the case where within a company group entities jointly process data in a centralised procedure. Again, in the end, it is always a question of the individual case that is to be checked thoroughly - usually with professional legal support as to the legal complexity of it.

Why is this question so important? Similar to what you just learned concerning Art. 28 GDPR (see for the contract that needs to be concluded in these cases below), Art. 26 GDPR requires joint controllers to enter into a specific agreement whereas the lack of it again might trigger objections by authorities and monetary fines. Such a contractual agreement must be

very transparent. It is mandatory to determine who fulfils which data protection obligations. In particular, who is responsible for exercising the rights of data subjects and who is responsible for information duties.

This is crucial as according to the GDPR any data subject can assert his or her rights against each individual (joint) controller, regardless of contractual distribution of tasks so that it is highly recommended for them to agree on certain rules and tasks to provide clarity!

If you don't have that particular agreement in place it is a violation of the law that can be sanctioned by regulators.

1.3.3 Processor – Who is a processor?

Being a controller imposes many obligations on the company. However, also being a so-called processor may lead to certain obligations under the GDPR.

A processor processes personal data on behalf of the controller and is a separate legal entity/individual with respect to the controller. According to Art. 4 No. 7 GDPR a processor can be a natural or legal person, public authority, agency or another body.

The controller has the choice of taking care of the data processing himself, assigning it internally to employees or departments, or outsourcing this task to external parties - a processor. Typical processors could be:

■ Examples

- Cloud computing suppliers
- Computing centres with (potential) access to personal data
- IT service providers
- Maintenance and support of software and IT services that do not necessarily include the processing of personal data but where (theoretical) access to such cannot be excluded.

As explained before, where a controller involves a processor there needs to be a specific agreement in place to cover the data transmission and processing by the processor. Art. 28 GDPR provides for very detailed requirements to be regulated in such an agreement, including the following points:

■ Art. 28 GDPR Contract Checklist

- Nature, purpose, object and duration of processing
- Type of personal data & categories of data subjects
- Scope of the powers of instruction of the person responsible
- Securing of technical and organisational measures
- Return or deletion of personal data after completion of order processing
- Control rights of controller vis-à-vis the processor
- Support of controller by contract processor in the event of inquiries and claims by affected parties and in the event of mandatory reporting of data protection violations
- Duty of the processor to provide information if instructions violate data protection law

Use the above as a checklist for designing such an agreement (you might often hear the term “Data Processing Agreement”). When doing so, be aware that European regulators and certain interest groups have published standard agreement templates that are worth

considering as a basis. However, please note that taking such a template “as is” will never do the trick. Remember: GDPR requires a risk based approach which also means that any Data Processing Agreement you are looking at needs to display the actual circumstances of the case at hand.

One more thing: As soon as the processor starts to determine his own processing purposes with the data, he himself becomes a controller to that extent and faces the obligations of a controller as well and will be liable such an a controller. In many cases, this may lead to difficulties as the processor usually will not have a legal basis to base the processing personal data fore own purposes on. If such a change of purposes is lawful will then be subject i.a. to Art. 6 (4) GDPR which governs the processing for purposes other then which personal data has been collected.

■ **Example:**

A processor receives personal data to process it solely on behalf of the controller (Art. 28 GDPR). The processor decides to use the personal data for big data analysis for its own business purposes. The latter would not be covered by the privilege awarded under the GDPR to data processors as the processor would exceed the scope of the “processing on behalf”. The processor would now i.a. need to present a legal basis for the processing (Art. 6 GDPR) and properly inform the data subjects on such a processing to give them i.a. a chance to object (see for example Art. 21 GDPR). In many cases a processor will not be able to meet these requirements and should, thus, treat these types of processing activities very carefully.

2 Processing personal data – How do I do it right?

So far we learned how to determine whether you are processing personal data in the meaning of the GDPR and if the GDPR applies to you given other relevant aspects.

But how do you make sure you comply with the requirements if they apply to you? The GDPR follows a simple but effective principle:

Every processing of personal data is forbidden, unless it can be legitimised.

This rule puts you in the often difficult position to ensure that all your processing activities are covered by a legal allowance ('legal basis') as set in the GDPR or other applicable laws. This to determine can sometimes be a rather complex process and will get to that in a minute. But even if you process data on a 'legal basis' that is not all you need to do. Furthermore, you will have to comply with the basic principles of a lawful data processing which we'll explain in more detail below. And - you guessed it - not just that: under the GDPR you also have to be able to proof that you comply with all these principles at all times which is then called 'accountability'.

So, let's get started!

2.1 When can I process personal data?

In order to being permitted to process personal data you need to determine a proper legal basis. A legal basis would be a rule in the law that tells you that in your particular or at least a similar case the law determines your processing legit. The main legal bases you usually consider when doing this check up are set out in Art. 6 para. 1 of the GDPR:

Art. 6 (1) GDPR

Processing shall be lawful only if and to the extent that at least one of the following applies:

- (a) the data subject has given consent to the processing of his or her personal data for one or more specific purposes;
- (b) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;
- (c) processing is necessary for compliance with a legal obligation to which the controller is subject;
- (d) processing is necessary in order to protect the vital interests of the data subject or of another natural person;
- (e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;
- (f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

Any processing without legal basis is considered unlawful and personal data collected without legal basis must not be used anymore and is to be deleted instantly. This also applies to any personal data that might have been collected lawfully under applicable prior laws (i.e. that have been legal under the prior law) while GDPR - due to its stricter approach - does not permit such a processing anymore.

So, in order to determine whether you can utilize one of the above “legal bases” for your particular processing we recommend the following checks:

■ **Checklist**

- ☑ Check if every processing of personal data is based on a legal basis.
- ☑ Regard that you might have several purposes you collect and process data for. In order to determine a proper legal basis you need to differentiate by the particular purposes and the personal data you process specifically for that purpose. A generic approach does not work under the GDPR. Remember: it’s a risk based approach!
- ☑ So, go through the list above per every set of data and every processing activity and apply one of the reasons provided for. If you easily can, you have a good chance to be in compliance with the law.
- ☑ If you have trouble to find a match for the purposes you wish to use personal data for, or if you are not sure about it, look for advice from your data protection officer or legal counsel.

While all of the above could be relevant to your processing of personal data, for sure the most relevant are:

- processing on the basis of consent (lit. a),
- necessary for the performance of a contract (lit. b) and
- processing on the basis of legitimate interest (lit. f).

The following deals with these main three legal bases. Let’s have a closer look at them:

2.1.1 When can I rely my processing on the Performance of a Contract?

The first and foremost important ground to receive and process personal data is usually the processing of personal data for the purpose of fulfilling (pre-) contractual obligations.

In many cases, the performance of contracts requires the processing of personal data. A restriction of these processing activities would make everyday life and business impossible, which is why the GDPR provides for a general legal basis for the processing of such data related to the fulfilment of contracts.

■ Typical Examples:

- The processing of the name and address of customers in relation to purchase contracts, e.g. for delivery or provision of a service, but not the gender or the shoe size of a person (as this is usually not required for performing the contract).
- Processing of billing information, in order to invoice customers; but if used for marketing purposes, these would again usually not be required to fulfil a contract and would therefore require another legal basis.

As you can see, the interpretation of the law is rather strict: in order to base processing on the performance of a contract, the processing must be strictly necessary to achieve the contractual goals. Processing for any other purpose outside of that scope will no longer be covered by that.

Secondly, the extent to which data is processed is limited to what is necessary for the fulfilment of the contract as other principles such as ‘purpose limitation’ and ‘data minimization’ apply.

■ **Example:**

When you sell goods or services online and customers need to register with your online shop you should limit the data collection to what is needed to perform the transaction. To ask for y birthdate might be interesting. However, usually that is no information you really need. If you want to collect it to send a birthday e-mail please note that this will usually be another “purpose” (usually related to marketing) and may, thus, require another legal basis other than “contract” .

Last but not least, after complete fulfilment of the contract (and its post-contractual obligations) there is no further legal basis for the ongoing storage of personal data. Therefore, the personal data has to be deleted (storage limitation) unless you can present another purpose in accordance with the GDPR. This is usually only the case under very narrow circumstances (see Art. 6 (2) GDPR). This means that once you collect personal data you should already have a strategy on how you get rid of it once the purposes you collected it for has ceased (e.g. the contract has been fulfilled).

In a nutshell, when assessing “contract” as a legal basis go through the following points:

■ **Checklist**

- ✓ Check if you have a contractual relationship with the data subject (e.g. purchase or service contract). If not, Art. 6 (1) (b) GDPR will usually not apply to you.
- ✓ Only collect as much data as you need to fulfil the contractual goal. Limit collected data to what is strictly necessary.
- ✓ Details matter - analyse your data very thoroughly and always evaluate the full picture! Remember: GDPR takes the risk based approach. This you will not be able to follow unless you know what you are doing!

2.1.2 What do I need consent for and how does that work?

If you don't have a contractual relationship with the data subject, consent might be a way to lawfully process personal data. Although consent is always a possibility to legalise your processing activities, you should proceed with caution as gaining consent might not only be commercially unfeasible, but might also bear certain legal risks. So, if you can, legitimise your processing activities on another legal basis, such as e.g. on legitimate interest (see below) only resort to consent if you don't have any other options.

This is all due to the strict requirements set forth by GDPR for obtaining valid consent and the fact that it can be withdrawn at any time. But let's go step by step:

First, valid consent needs to meet the criteria as provided in Art. 7 GDPR:

■ What are the basic requirements?

- Must be freely given: The data subject needs to have the choice; usually no bundling allowed with e.g. the offering of services which are against payment; exemptions are possible but very rare!
- Can only be obtained for one specific purpose: Including several purposes into one consent usually requires that the data subject has a choice to opt for all or just some of them.
- Needs to be very transparent: Presented in a manner which is clearly distinguishable from other matters, in an intelligible and easily accessible form, using clear and plain language
- Be clear - indicate the purpose of processing, the personal data used and the participating entities ;
- Prior to giving consent, the data subject shall be informed on its right to withdraw the consent and what consequences it might have.

Whether consent is freely given, depends on each individual case. Any prospect of disadvantages to the data subject might hinder the assumption of a freely given consent. This is particularly critical in employment contexts as employees often give their consent because they have to in order to safeguard their position. As a result, such consent is usually not given freely.

■ Example

You want to publish your employees' pictures on your company's website to show customers your team. This is usually something that requires consent.

Depending on how you design the procedure asking for consent, it might not be deemed valid as employees might not have a real choice.

A solution to this problem might be to offer employees the chance to consent (or not consent) without any adverse effects for them. This would then be freedom of choice! If you ensure that you should be ok. In any case, ensure the employee is informed about all aspects of the processing (Where is the picture visible, to whom and for how long?).

Please note that consent must be obtained separately for each purpose, meaning that you would need for example offer a form with several checkboxes if you wish to process personal data for several purposes based on consent (no bundling allowed).

■ Example

You want to send your customers marketing e-mails but you would also like to share personal data of your customers with partner companies for other reasons. If you aim at obtaining consent from the data subject for that this would require you to apply for example two separate checkboxes on a consent form.

As we learned about accountability already don't forget that you need to document the obtaining of a proper consent. So, if you receive it electronically provide for a way to have it in reach once needed to prove you are in compliance with the law. If you can't it might be that a regulator (or court for that matter) might deem you in breach of the law just because of that! So, always think of a way not only how to obtain it but also how to prove it afterwards!

Lastly, be aware that consent can be withdrawn at any time. In that event, personal data processed on the basis of this consent would need to be securely deleted or anonymised. After withdrawal of it a further processing - at least if based on the consent would not be permitted anymore! Be aware: there is (almost) no limit for a data subject to withdraw a consent.

Please also note that a certain age limit for granting valid consent might apply in your jurisdiction. For example, if you sell goods or services to children obtaining valid consent might be an issue. If you do, always obtain specialised advice as this is usually a rather complex legal issue.

If you don't abide to the aforementioned requirements consent might be deemed invalid and, as a consequence, lead to unlawful processing of personal data.

In a nutshell, when checking consent as a possible legal basis work along the following points:

■ **Checklist**

- ☑ Always strongly consider if you really need consent or not - it's the least practical solution. Consider other options first (see above)!
- ☑ When obtaining consent use a clear and unambiguous language. Be precise and provide for transparency. Otherwise there is a high risk that your consent might be invalid - and so will your data processing be!
- ☑ If you already obtained consents prior to May 2018 (GDPR) check if consent is necessary and if it was gained lawfully. If an "older" consent does not comply with the GDPR requirements it is invalid. Again if you are not sure, look for advice from your data protection officer or external legal advice.
- ☑ Last but not least, ensure a process to be in place in case consent is withdrawn or invalid (i.e. deletion procedures for such data).

2.1.3 When do I have a legitimate interest to process personal data?

The GDPR further allows processing of personal data on the basis of legitimate interests on your or another third party's side. This means, that the law acknowledges that there are sometimes individual interests that are hard to be put into a specific rule in the law.

■ **Example**

Checking your business partner's solvency might serve as a legitimate interest as this is something that can be reasonably expected by the parties.

Whether your respective interest is legitimate and might prevail against the interests of the data subject depends on the individual case. It needs to be decided (and documented) on a case-by-case basis.

The age of the data subject, intimacy of personal data or existence of a special category of personal data might serve as indicators in order to perform the balancing test which is required to weigh to the interests. The following typical indicators might help you with your assessment:

- If special categories of personal data (e.g. information on physical or mental health) are processed, interest of the data subject might more likely overrule other interests.
- If the personal data is already accessible online, even trivial interests may override the interests of the person in question.
- One of the most important indicators would be the expectation of the data subject with regard to a certain processing of data. E.g., an EU user might expect that his website usage behaviour will be analysed but might not expect that a profile is created and sold to third parties.

As a rule of thumb, the greater the implications to the privacy of the data subject, the more important your interests need to be.

For example, solely financial interest might be weaker than the interest of providing a stable and secure service.

GDPR defines certain legitimate interests, which are of high importance for day to day business operations, including the legitimate interest to conduct direct marketing activities or to transfer personal data within a company group for administrative purposes. Keep in mind though that those provisions must - again - be interpreted rather strictly.

If you have the chance to choose,, processing on the legal basis of performance of contract should be preferred (if applicable), as data subjects might have a right to object against the processing based on legitimate interest (Art. 21 GDPR).

■ Checklist

- ☑ When considering “legitimate interest” as a legal basis Check if you can process personal data on any other legal basis (in particular on the performance of contract).
- ☑ When relying on legitimate interest consider your and the data subjects interest properly: the more sensitive a processing activity, the more likely that the data subjects interest in you NOT to process his/her personal data may overrule your intentions.
- ☑ Document such consideration (e.g. in your record of processing activities) as supervisory authorities might ask for it. Remember: you need to proof your compliance which includes a proper documentation!

2.2 Processing special categories of personal data – What is special?

Now that we have learned how to determine whether you have a legal basis or not for your processing you need to learn that certain data categories require further safeguards and are to be treated differently.

Although the GDPR protects all personal data, some data is protected in a special way. According to Art. 9 GDPR there are special categories of personal data, such as data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person’s sex life or sexual orientation,

Art. 9 GDPR therefore lays down stricter requirements and even puts a fundamental ban on the processing of such sensitive data (Art. 9 (1) GDPR). According to Art. 9 (2) GDPR,

exceptions are conclusive and only allowed under very narrow circumstances, as these kinds of data are particularly sensitive and therefore particularly worthy of protection. Otherwise, there are considerable risks to fundamental rights and freedoms for the data subject if these data are not carefully processed and protected against misuse. This is to ensure that data subjects are not discriminated against on the basis of their religion, political opinion or state of health. Be it by authorities, employers, insurance companies or other bodies.

As a rule of thumb, processing of special categories of personal data will require explicit consent of the data subjects unless processing occurs in the course of specific business fields, e.g. where strictly necessary to perform medical treatments or if needed to allow necessary processing of personal data within the employment relationship. Processing based on legitimate interests in the meaning of Art. 6 (1) (f) GDPR is usually not possible. As to the high sensitivity of the processing activities and the damage that can be done when special categories of data are used in a non-compliant manner, it is highly recommended to thoroughly check along the rules set forth in Art. 9 GDPR.

Acting as a processor in the meaning of Art. 28 GDPR and processing special categories of data on behalf is not per se forbidden. However, data protection authorities tend to be very strict when evaluating these types of business models and require a certain level of technical and organizational safeguards, e.g. with regards to the requirements for respective agreements.

To summarize the message: When dealing with special categories of personal data be very careful with it and assess the legal circumstances very thoroughly. The following checklist may serve as a start but always discuss these with you data protection officer and legal advisor.

■ Checklist

- ☑ When processing involves special categories of data be aware of the specific requirements GDPR sets for it!
- ☑ Always strongly consider if you really need to obtain these types of data; if not it makes life a lot easier for you.
- ☑ If you need to process these types of data look for a legal basis in Art. 9 (2) GDPR and consider that even though you find one further rules may apply according to the GDPR or national laws which are also binding.
- ☑ When you outsource certain processing activities to third parties which include the processing of special categories of personal data thoroughly evaluate the requirements you have to meet to do so. If you are, for example, providing IT services to a hospital and might have access to patient data these operations will be permitted by law under very narrow circumstances only. These should be made subject to a detailed review with specialists on data protection and other laws concerning the processing of patient data.
- ☑ Please note that in some countries unlawful access to these types of data might even be punishable by criminal law. One more reason to take a closer look at it at an early stage!

3 What other principles do we have to observe when processing personal data?

At this point we might have found out about your “role” when processing personal data and ideally a proper ‘legal basis’ to do so. But that is not enough as we will see.

Further, you always have to comply with the basic principles of a lawful data processing, which are in short:

- Fairness and Transparency
- Purpose Limitation
- Data Minimisation
- Accuracy
- Storage Limitation
- Integrity and Confidentiality

These principles apply in parallel and under any circumstances. So, get familiar with these principles before starting to process personal data under the GDPR.

And one more thing: Yes, of course non-compliance with one of these aspects might trigger an authority sanction such as a monetary fine. There are usually no de minimis violations in the GDPR, so that authorities usually have to sanction any type of violation. The following principles are not just “nice to have”, they are essential requirements that require action!

3.1 Transparency under the GDPR – What is required?

Under the GDPR all forms of processing are subject to transparent information of the data subject on the processing of its personal data. Data subjects need to receive information on all relevant aspects of a processing activity. In short: They always have to know if you have their personal data in their possession, why and what you are going to do with it. Even if you receive personal data not directly from the data subject but from third party sources (e.g. publicly available websites) these principles will apply nevertheless and may require you to inform the data subject anyways.

As a general rule, data subjects need to be provided with the following information when collecting of their data. Art. 13 GDPR may serve as a checklist therefor:

- Identity of controller (usually entity name, address, contact details and representatives)
- Contact details of the Data Protection Officer of the controller
- Processing purposes and legal basis (in short: why you have it and what you do with it)
- Legitimate interest if levied pursuant to Art. 6 (1) (f) GDPR
- Recipients of personal data during transmission (e.g. a service provider)
- Transfer to third countries such as Korea (e.g. parent company located there)

According to Art. 13 (2) GDPR the controller must also provide the following information

- Duration of storage (e.g. how long you intent to keep the data and why)
- Rights of data subjects (e.g. rights to object to the processing)
- Revocability of consent (where consent has been given)
- Right of appeal to supervisory authority (Art. 77 GDPR)
- Obligation to provide personal data e.g. for conclusion of contracts
- Automated decision making and profiling

Non-transparent processing activities might be found invalid and therefor forbidden. As to a strict view of the authorities the entire processing might be illegal. So, better spend some time on being transparent to avoid negative consequences.

As already explained, data subjects must be informed at the time of survey, this means when data is obtained. This is mostly done within a 'privacy policy' that you provide to data subjects (e.g. your customers, employees or business partners), describing on how you use their personal data in the business relationship. It can be done in writing (e.g. on a piece of paper) or electronically (e.g. on a website). In theory, it might also be possible to provide necessary information orally. However, this is usually not recommended as you will have a

hard time to proof your compliance as there will typically be no documentation. This might be different when you run a call center and decide to include information according to the law into your procedures (e.g. with automated computer-based read outs or references to further documents e.g. on the internet). If you are concerned with these types of processing a detailed review and proper legal advice is necessary as the requirements are still very much under discussion in Europe.

As privacy policies are a very common way of complying with these requirements, the obligation to provide such information does not only apply to online procedures - where the use of a privacy policy is even common today - but also for any offline procedures. Such a policy needs to address the above points in a transparent manner while information does not need to be provided in a specific format and could, thus, also be provided e.g. to customers with an information sheet attached to a service contract as long as you chose a most transparent way to present the information.

If you obtained data from third party sources (e.g. another controller or a publicly available website) and not directly from the data subject further information obligations apply. Amongst others the controller needs to inform the data subject on how it obtained the data (see Art. 14 GDPR for details). The rules are different to those that apply when you deal with the data subject directly (see Art. 13 GDPR). When this applies to you - again - you need to thoroughly assess what is needed.

So, what's to take away for transparency? The following checklist may provide a first overview and guidance:

■ Checklist

- ☑ Check if you are subject to information obligations. This will be the case almost every time. Exemptions will be interpreted in a very narrow manner.
- ☑ If so, set up sufficient privacy policies and notices and ensure a process to provide these to the respective 'data subject'.
- ☑ Inform on all relevant aspects and use Art. 13 and 14 of the GDPR as a Checklist to complete the forms with all necessary information.
- ☑ If it doesn't hurt always provide rather more than less information.
- ☑ Regard that your customers, employees or business partners are no legal experts. Use a clear, unambiguous and precise language.

3.2 Purpose Limitation and Data Minimization - What's to be done?

Personal data can only be processed for a certain purpose and that processing for the specific purpose must have a legal basis.

In case data is processed for other purposes than the ones it has been obtained for in the first place (e.g. fulfilment of contract and subsequent use for marketing activities) each purpose must be legitimised through a separate legal basis. As a consequence, a change of purpose is generally only legally permissible when:

- it can be based on the data subject's consent (see IV.4); and/or
- the new purpose is compatible with the initial purpose.

■ Example

You collect the e-mail address of a customer in order to inform customers on their purchase. Furthermore you want to use the e-mail address for marketing purposes (e.g. sending of newsletters).

While the first purpose (information on specific purpose) can rely on the performance of contract legal basis, the second purpose (sending of newsletters) cannot, as this is not related to the performance of contract. Therefore a separate legal basis would be required (e.g. consent).

In addition, the principle of data minimization applies to all processing activities meaning that only that data shall be processed that is required for the specific purpose. This principle gets often forgotten in form situations, i.e. situations where personal data is collected via an online form. For example, it will generally not be necessary to ask for the age or gender on a simple contact form and as a result such data collection could be considered unlawful. As a consequence, such data would need to be erased. Also, once you start to design a data deletion concept (meaning a concept guiding you in removing data from your systems) especially the data that has been collected ignoring the data minimization principle will cause trouble. So, limit the amount of data you are collecting in the first place and make your life easier!

■ Checklist

- Check what personal data you really need to reach your goals.
- Collecting personal data just because you CAN is not a reason and will get you in trouble!
- Instruct your employees to act accordingly.

3.3 Accuracy and Data Subject's Rights - How do we ensure that?

Personal data shall be accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay.

■ Checklist

- ✓ Check what personal data you really need and erase old and inaccurate data promptly to limit redundancies and provide for proper data quality.
- ✓ If a data subject wishes to correct or have access to his/her data (e.g. because of a new name or address) react promptly and ensure business processes accordingly.
- ✓ Set up sufficient policies and instruct your employees accordingly to ensure high service quality.

3.4 How is the storage of personal data to be limited?

When you no longer need the personal data for the purposes for which it was collected in the first place, the data must either be securely deleted or destroyed, or fully anonymised.

In order to do so, you must:

- evaluate the length of time you usually need to keep personal data and for what purpose, and
- securely delete information that is no longer needed for a specific purpose.

When determining proper periods for allowed data storage, local laws and the imposed specific minimum and maximum retention terms might serve as a first indicator. For instance, retention terms in relation to tax records, health records of employees and documents relating to a dispute or litigation.

In order to comply with the principle of accountability you should document your data retention plans in a retention policy and regularly check and update it. To work towards it the following steps should be taken:

■ **Checklist**

- ✓ Find out where you store personal data.
- ✓ Determine how long you need personal data (retention period) while these periods might differ depending on the categories of data and business purposes you collect-ed them for in the first place. Local laws might serve as orientation when it comes to determine compelling storage periods (e.g. for archiving required by law).
- ✓ Delete data that is no longer needed for a specific purpose in a timely and secure manner or design procedures to doing so automatically if you can.
- ✓ Set up a sufficient data retention policy that documents the aforementioned.

3.5 Ensuring Integrity and Confidentiality - How do we do that?

To protect personal data from unauthorized access, loss, theft or damage, you must implement adequate technical and organizational security measures. IT systems shall be designed in a way that the above goals shall be met.

When doing so you need to take into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons. The safeguards taken need to ensure a level of security appropriate to the risk, meaning that the law does not allow a “one-catch-all” approach but rather requires companies to design individual procedures and safeguards to ensure proper IT security.

For further details please see below under Section 6.

3.6 Privacy by Design and Privacy by Default - What is that all about?

The GDPR takes the existing security requirements to a further level and incorporates preventive mechanisms such as the principle of 'privacy by design' and 'privacy by default'.

According to the principle of privacy by design, your business processes shall be designed in a way to adhere to the principles laid down in the GDPR, e.g. by limiting data collection in the first place. Processes need to be designed in order to minimize data streams and prevent - where possible - the processing of personal data e.g. by means of anonymisation. Privacy by Design requires companies to start to look at GDPR right from the start of the development process, e.g. together with IT developers in order to implement safeguards.

Privacy-by-default requires controllers to implement appropriate technical and organisational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed. Similar to privacy-by-design, privacy-by-default requires controllers to involve data protection advice and design at an early stage of the development process whereas the focus will be to collect lesser amounts of personal data, to reasonably limit the extent of their processing and to shorten the period of their storage and their accessibility as far as possible through respective data protection friendly pre-settings of a service. So, privacy has to become the default option, not the other way around!

3.7 Privacy Impact Assessment - What is it and when to conduct one and when not?

Another preventive mechanism that GDPR introduces would be the controller's obligation to perform a so-called 'privacy impact assessments' (or PIA), a pre-assessment of a planned procedure to assess, ensure and document its GDPR compliance before its enactment. To conduct a PIA is necessary in specific cases which usually indicate higher risks to the rights and freedoms of natural persons, especially where new technologies are used to process personal data.

A PIA will be required where a controller performs

- (i) procedures including automated decision making and profiling which means processing activities that entail (a) a systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing, including profiling, and (b) on which decisions are based (c) that produce legal effects concerning the natural person or similarly significantly affect the natural person (e.g. credit rating based on automated processing and an automated rejection of a loan contract based on the rating);
- (ii) processing on a large scale of special categories of data referred to in Article 9 (1) of the GDPR (e.g. health data), or of personal data relating to criminal convictions and offences referred to in Article 10 of the GDPR; or
- (iii) a systematic monitoring of a publicly accessible area on a large scale (e.g. where CCTV is applied).

The European data protection authorities have published several guidelines with remarks on the relevant cases which will be updated constantly and should therefore be considered when evaluating conducting a PIA or not (for further details please see Section VI, below).

■ Examples

- Any processing activity that involves profiling (automated decision-taking on the basis of data subject' s personal information, e.g. credit checks, loan applications)
- Use of innovative technologies such as Cloud Computing or Big Data
- Large scale processing of Article 9 & 10 data (e.g. political parties membership data, health records processed by hospitals, gyms, health centres; dating websites/ applications)
- Systematic monitoring of a publicly accessible area, e.g. showrooms or similar, on a large scale (e.g. CCTV)
- Monitoring of your employees behaviour

Where one considers a PIA to be necessary, the PIA needs to cover and document the following aspects:

- (i) a systematic description of the envisaged processing operations and the purposes of the processing, including, where applicable, the legitimate interest pursued by the controller;
- (ii) an assessment of the necessity and proportionality of the processing operations in relation to the purposes;
- (iii) an assessment of the risks to the rights and freedoms of data subjects referred to in the relevant provisions of the GDPR; and
- (iv) the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with the GDPR taking into account the rights and legitimate interests of data subjects and other persons concerned.

Processors will usually not have to conduct a PIA for procedures they operate on behalf of a controller. This might be different where processing of their own employee data is in question.

In the end, to determine whether you need a PIA or not you could follow these basic points:

■ Checklist

- Go through the list of your processing activities and try to locate possible high risks
- To assess the level of risk, you must consider both the likelihood and the severity of any impact on individuals (high risk can result from either a high probability of a lower level of harm, or a lower possibility of grave harm).
- Your PIA must include:
 - A description of the nature, scope, context and purposes of the processing;
 - An assessment of necessity, proportionality and compliance measures;
 - An identification and assessment of risks to individuals; and
 - An identification of any additional measures to mitigate those risks.
- Thoroughly document every step

4 Rights of the Data Subjects – What are my obligations?

Even if you process personal data on legal bases and comply with the principles of lawful processing, if a data subject exercises its rights, you have to ensure that their requests are promptly met.

Why is that? Because GDPR has strengthened data subject's rights and raised awareness! Under the GDPR, more and more customers or employees will for example ask for access to or erasure of their personal data e.g. after a business relationship or an employment has ended.

Your data processing and relevant systems need to provide the option to ensure accuracy and for example allow for an easy way to modify personal data accordingly where legally required.

In order to be able to react to respective requests companies need to establish procedures and technical and organizational measures to be able to respond to and comply with any such requests within reasonable time. These rights can be exercised freely and must generally be met within 30 days.

4.1 Right to Access

The right to access is regulated in Art. 15 GDPR. Once you receive a request for access you need to be able to figure if you hold data relating to that particular person at all and inform the requesting person on it (Stage 1). If the answer is yes, the data subject is entitled to the following further information (Stage 2):

- A copy of the personal data, e.g. by providing a list of data you hold with regard to the data subject
- Further “metadata” such as the purposes of processing and categories of personal data and timeline for data storage
- Information on data subjects rights to deletion, rectification and restriction
- Right to file a complaint to the supervisory authority
- Information on the source of data (e.g. a website etc.)
- Information on personal data is transferred to third parties
- If automated decision-making is used
- Information on the receivers of data

There is no specific form for providing this information. However, in the end you’ll have a great interest in properly documenting what you disclosed to being able to proof your compliance.

Given the fact that the law leaves you a very narrow timeline to comply with the request - usually for Stage 1 approximately 4 weeks and another four to eight weeks for Stage 2 - you'll need to establish a functioning process to find personal data and to properly disclose the information to the data subject.

Please keep in mind that you might also need some time to evaluate if a requesting party is authorised. Thus, you need to make sure that you do not disclose data to unauthorised individuals,

4.2 Right to Erasure, Rectification and Restriction

These rights, as laid down in Art. 16, 17 and 18 GDPR, pursue the purpose to prevent or revoke violations of the law by the controller. They tend to be the most effective for the data subject. The right to erasure applies where personal data has been collected and processed lawfully, or where the purpose has been omitted. The right to rectification specifies the principle of accuracy, the data processed shall reflect the reality. The right to restriction of processing as laid down in Art. 18 GDPR, pursues the scope to balance the interests of both, the controller and the data subject.

The right to erasure usually requires controllers to completely erase personal data when requested so in a legitimate manner. The mere blocking of data may not be a sufficient measure to comply with Art. 17 GDPR,

■ Checklist

- ☑ In order to comply with erasure requests effectively you need to have a process in place.
- ☑ Train your employees on how to deal with such a request properly and in a timely manner.
- ☑ Establish your systems accordingly in order to be able to fulfil a request, i.e. to find a person's data and to properly erase it when needed.

4.3 Right to Data Portability

The right to data portability under Art. 17 GDPR represents one of the few absolute innovations in the rights of data subjects. This right is intended to ensure that the data of the data subject can be transferred from one controller to another controller. The purpose is to make him economically more flexible and ensure more competition among service providers processing personal data. However, this is not a uniform law but a bundle of obligations and claims. The data subject has a right to receive data and a right to direct transmission of his personal data in a certain format. There must be four cumulative conditions for an entitlement: The data subject's personal data must be processed. This processing must have been automated and the data must have been provided by the data subject on the basis of consent or contract.

In practice it is quite difficult to assess which data is to be provided hereunder and what is not. If you are in a field of business where it is likely that customers change the service provider regularly and might wish to take their personal data with them to ease the onboarding with that new service provider you need to evaluate this in more detail than others. Please also note that lots of details concerning the right to data portability are still under discussion.

So, monitor developments closely!

4.4 Right to Object

The right to object under Art. 21 GDPR serves to protect the special interests of the data subject in the case of lawful processing within the meaning of Art. 6 I lit. e and f GDPR (mostly when based on legitimate interests). Consequence of the objection is that the processing must be terminated and the data deleted if the data subject brings forward grounds relating to the particular situation which might render the processing illegitimate. However, if the controller demonstrates compelling legitimate grounds for the continued processing which override the interests, rights and freedoms of the data subject or where processing is necessary for the establishment, exercise or defence of legal claims the controller might continue.

If the controller uses the data for direct marketing purposes, Art. 21 II GDPR grants such a right irrespective of the legal basis of processing so that the controller will have to comply with such a request in any case - an approach that should be typical in many countries.

■ Checklist

- Familiarise yourself with the right of the data subjects to object!
- Implement a mechanism to ensure the rights of the data subject are met promptly upon request and in particular in time!
- Train your staff accordingly!
- Never ignore a request - otherwise it might become hard to handle!

5 Accountability and Documentation – What’s required under the GDPR?

Now that you process data on a ‘legal basis’ and further comply with the basic principles of lawful data processing, you have to provide proof of the compliance with applicable laws (‘accountability’).

Upon request of supervisory authorities, controllers must be able to prove their compliance as they carry the burden of proof. The controller’s records of processing activities will be helpful - and required by law - as details on the entity’s data flows will be included in them. It needs to be maintained either in writing or in electronic form and shall be made available to the authorities upon request.

The records of processing activities of a controller will have to display the following basic information with regard to certain processing activity:

- the name and contact details of the controller and, where applicable, the joint controller, the controller’s representative and the data protection officer;
- the purposes of the processing;
- a description of the categories of data subjects and of the categories of personal data;
- the categories of recipients to whom the personal data have been or will be disclosed including recipients in third countries or international organisations;
- where applicable, transfers of personal data to a third country or an international organisation, including the identification of that third country or international organisation and, in the case of transfers referred to in the second subparagraph of Article 49 (1), the documentation of suitable safeguards;
- where possible, the envisaged time limits for erasure of the different categories of data;
- where possible, a general description of the technical and organisational security measures referred to in Article 32(1).

The records of processing activities of a processor follow similar aspects but will require the following contents:

- the name and contact details of the processor or processors and of each controller on behalf of which the processor is acting, and, where applicable, of the controller's or the processor's representative, and the data protection officer;
- the categories of processing carried out on behalf of each controller;
- where applicable, transfers of personal data to a third country or an international organisation, including the identification of that third country or international organisation and, in the case of transfers referred to in the second subparagraph of Article 49(1), the documentation of suitable safeguards
- where possible, a general description of the technical and organisational security measures referred to in Article 32(1).
- security measures referred to in Article 32(1).

As the obligation to maintain a record of processing activities may be resource and time consuming especially for small and mid-sized companies GDPR provides for a de minimis criteria as to which companies may be exempted to maintain the register. According to Art. 30 (5) GDPR, an enterprise or an organisation employing fewer than 250 persons will not be obligated accordingly unless the processing it carries out is likely to result in a risk to the rights and freedoms of data subjects, the processing is not occasional, or the processing includes special categories of data as referred to in Article 9 (1) GDPR or personal data relating to criminal convictions and offences.

In short, no matter how large your organization is: once you perform sensitive processing activities you will need to implement a register anyways.

Furthermore a register of processing activities should only be the core of a more advanced Data Protection Management System (DPMS), which should be implemented, where proportionate. A DPMS is an internal compliance system and can be based on already existing compliance systems or combined with them to streamline existing procedures. When looking on how to document your processing of personal data according to the GDPR the following checklist should provide first guidance:

■ Checklist

- Widely document any decisions and processes incorporated in accordance with data protection compliance.
- Check your documentation along the existing rules in the GDPR (Art. 30 GDPR) and samples / best practices available from regulators.
- Implement mechanisms and procedures for monitoring and maintaining the register up to date.
- Enhance awareness for data protection (i.e. workshops, training...).
- Ask your data protection officer or legal counsel for help, if required.

6 Technical and Organisational Measures - What measures do I have to take?

Art. 32 GDPR obliges the controller and processor to implement appropriate technical and organisational measures (TOM) in compliance with data protection. It should thereby be taken into account the nature, scope, context and purposes of the data processing and the risk to the rights and freedoms of individuals. As you can see the law requires a risk-based approach towards data security which will require the involved stakeholders to evaluate a technical and/or organizational measure to be appropriate in the individual situation,

The law lists the following measures to be taken in order to reduce potential risks for data subjects or other involved parties:

- (i) the pseudonymisation and encryption of personal data;
- (ii) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
- (iii) the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident; and
- (iv) a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

As to the very generic wording of the GDPR many companies struggle with what really needs to be done here. Some of the most common measures that are to be taken in day-to-day business may include:

- Data processing systems are not used without authorisation, (e.g. by using appropriate passwords).
- Persons entitled to use a data processing system have access only to the data to which they have a right of access (e.g. by means of an access management system).
- Personal data cannot be read, copied, modified or removed without authorization in the course of processing or during electronic transmission (e.g. by data encryption).
- It is possible to check and establish whether and by whom personal data have been put into data processing systems, modified or removed (e.g. by file protocols).
- Personal data is protected from accidental destruction or loss (e.g. by back-ups or disaster recovery plans).

In any case, what is required by law always depends on the level of risk created through the processing. It might be more significant where sensitive actions take place with regards to for example special categories of personal data.

What you learned during your assessment then needs to be fixed in a data security concept which could follow a classification of your data processing activities along the sensitivity of the processing activities and documents your approach to ensure a proper level of security and integrity of the data.

In order to proof your concepts and how people comply with it you need to establish regular trainings and workshops to raise employees' awareness and implement regular controls and tests to ensure the proper quality and effectiveness of your measures.

7 Data Protection Officer – Do we need to appoint one?

Depending on the kind of processing and the category of personal data you might be obliged to designate a Data Protection Officer (DPO).

7.1 What is the role of a Data Protection Officer?

The tasks of the DPO are set forth in Art. 39 GDPR and include at least the following:

- inform and advise the management and employees on obligations under the GDPR;
- monitor compliance with all data protection provisions and own policies in relation to the protection of personal data, including the assignment of responsibility, awareness-raising and training of staff involved in processing operations, and related audits;
- the DPO also cooperates and manages communications with the data subjects and the supervisory authorities.

The DPO must be independent and he/she only reports to the highest management. Also, make sure that he/she is an expert in data protection and adequately resourced so that the tasks can be carried out properly. You can choose the DPO from your own personnel or you can hire one externally.

7.2 Are we obliged to designate one?

Under the GDPR, you are usually obliged to designate a data protection officer when you are a very big company with more than 250 employees. However, in the following cases you have to appoint a data protection officer in any event: either when (1) your core activities consist of processing operations which, by virtue of their nature, their scope and/or their purposes, require regular and systematic monitoring of data subjects on a large scale (e.g. video surveillance or internet tracking); or (2) your core activities consist of processing on a large scale of special categories of data (e.g. health data).

In addition, local laws might provide further situations in which the designation of a data processing officer is required (usually depending on the size of a company; in Germany for example starting at currently 10 employees, maybe more once new legislation has been approved).

Please note, a data protection officer does not take over any liabilities for your actions (besides under general civil/employment law, e.g. under delict/tort). The data protection officer only controls what the company does in terms of data protection. In order to set him / her into the position to do so you need to provide proper resources and involve him / her into your business decisions where it affects data protection.

Important for Korean companies: If you are located on Korea and you are subject to the GDPR it might well be that you need to appoint a data protection officer as well. A place of business does not prevent you from having a DPO.

■ Checklist

- Check if you are obligated to designate a data protection officer according to GDPR or national laws. In some countries, the rules are stricter. If you are not sure please contact local legal counsel to check.
- If needed, designate a DPO who conforms to the rules of the GDPR.
- Document the appointment properly.
- Allow the DPO to support your organisation - don't keep him/her out!

8 Transfer of Personal Data to third parties What do I need to observe when allowing others to access personal data?

When managing external flows of personal data there are important things to consider: the transfer of personal data to others is - as indicated above - also considered 'processing', meaning that any transfer of personal data to a third party outside your organisation needs to be transparent and based on a legal basis. Please note that making data accessible to others while it still remain under your control will also be considered a transfer. We look into examples for that in more detail below.

8.1 Transfer of data to group companies - no intra-group privilege

In this context, third party also means any company of your company group that you might be associated with as the law does not provide for a general privilege to freely transfer personal data in a company group (no intra-group privilege). Hence each group entity will be accountable for its own data protection compliance.

In order to transfer data within your company group, a few typical measures and safeguards have proven practical to ensure GDPR compliance, foremost to design and establish data processing agreements within your company group (see below). Also, GDPR acknowledges that there are certain privileges for company group data transfers when concerning administrative support or the like. The boundaries are not established yet but there are good arguments to say that company group transfers might - at least to a certain extent - be based on legitimate interests (see Art. 6 (1) f) GDPR). Once you are facing this issue get specialised advise from your DPO and legal counsel to define the proper safeguards.

8.2 Transfer to processor - data processing agreement required

Data processors such as a hosting service provider that operates your company's IT systems on your behalf or maintains and supports specific software products are - from a data protection law perspective - to be seen as a part of your organisation. Therefore the transfer of the personal data to it does not require a separate legal basis such as the data subjects consent.

Main requirement for the use of data as a processor is, however, the conclusion of a data processing agreement in accordance with Art. 28 GDPR (see above under Section 2 for details).

8.3 Transfer of Personal Data outside the EU/EEA

Another issue is the transfer of personal data outside the EU/EEA, or more precise the transfer of personal data into a country with non-adequate data protection safeguards. The GDPR requires in these cases appropriate alternatives to ensure a minimum standard of data protection safety.

GDPR provides for several ways on how this can be achieved. Once a country is deemed a safe country in the meaning of Art. 45 GDPR the transfer to such a country would not require additional measures than those already covered above (e.g. to conform to Art. 5 and 6 GDPR). In a nutshell, you always have to ask whether there is a valid legal basis according to Art. 6 of the GDPR and if you comply with the additional requirements set by GDPR to transfer personal data internationally (Art. 44 GDPR).

This might be best displayed with the following example:

■ Example

You as a European enterprise are using a service provider for IT maintenance services in Korea who has access to your customer's personal data. The service provider would, most likely, be regarded a processor. Therefore, a data processing agreement would have to be concluded (see Art. 28 GDPR). Furthermore, since the service provider has its seat outside the EU in a country where no adequacy decision of the European Commission exists, in addition to the data processing agreement other measures acc. to Art. 44 GDPR would be required, e.g. through the conclusion of Standard Contractual Clauses.

Means typically used are the so-called EU Standard Contractual Clauses, a set of model clauses designed by the European Commission to be concluded between the parties of an international data transfer. Another option would be the so-called Binding Corporate Rules. These are specific contracts which have been negotiated with European regulators to cover international data transfer and have been approved by them.

When looking at the different options to cover international data transfer these would be the typical questions to ask:

■ Third Country Transfer

- Is transfer to a country covered by a so-called Adequacy decision (e.g. for “Safe Country” such as Israel or Canada; please note that a Privacy Shield Certification for the US would also fall into this scope)?
- If not, will it be possible to enter into the so-called Standard Contractual Clauses, a set of model clauses to be concluded between the parties and provided by the EUC to legitimise the transfer abroad? If so, this would be a typical and often most practical solution.
- If that’s not an option, is there an accepted special contract by competent supervisory authority (not relevant for your business)?
- Another alternative would be enacted Binding Corporate Rules. Do you have those?

Typically, when involving processors outside the EU / EEA most companies aim for concluding the above mentioned Standard Contractual Clauses to be executed to cover the data transfer. When using those please consider that there are several sets of model clauses which you can find on the websites of the European Commission. Some of them refer to so-called “controller-to-controller” transfers and will, thus, not be the right choice if you involve a processor abroad. Again, ask your DPO or legal counsel which set of documents matches your situation.

9 What are the consequences of non-compliance?

Now that we gained a good overview on what needs to be done it is time to learn about what happens if you are not on compliance.

Non-compliance with data protection and related obligations may result in liability and penalties. The types of liability and penalties in a country are foreseen by law and typically consist of:

- civil liability (following claims for data subjects or class actions);
- criminal liability (criminal fines, imprisonment, etc.);
- administrative liability (administrative actions including warnings and fines); and
- reputational damage for the company.

Please note that under GDPR infringements can be subject to administrative fines up to EUR 20 million or in the case of an undertaking, up to 4 % of the total worldwide annual turnover of the company group in the preceding financial year, whichever is higher.

Administrative fines will depend on the circumstances of each individual case. When deciding whether to impose an administrative fine and deciding on the amount of the administrative fine in each individual case due regard shall be given by a data protection authority to i.a. the following criteria:

- (i) the nature, gravity and duration of the infringement taking into account the nature scope or purpose of the processing concerned as well as the number of data subjects affected
- (ii) the intentional or negligent character of the infringement;
- (iii) any action taken by the controller or processor to mitigate the damage suffered by data subjects;

- (iv) the degree of responsibility of the controller or processor taking into account technical and organisational measures implemented by them pursuant to Articles 25 and 32;
- (v) any relevant previous infringements by the controller or processor,
- (vi) the degree of cooperation with the supervisory authority, in order to remedy the infringement and mitigate the possible adverse effects of the infringement,

The listing shows how important it is to deal with authorities in a constructive and collaborative manner and to prepare towards GDPR compliance.

10 Working with the supervisory authorities

According to Art. 31 GDPR you have to cooperate with the relevant supervisory authorities upon request. But since each EU Member State has its own national Supervisory Authority - some member states even have several of them such as Germany where you find 17 different data protection authorities - and processing activities nowadays more often have transnational dimensions, taking place in different EU member states and / or affecting individuals from different countries, it can be difficult to determine the competent Supervisory Authority.

Authorities have investigative and corrective powers which are further set forth in Art. 58 GDPR. If needed they could for example carry out investigations in the form of data protection audits or obtain access to all personal data and to all information necessary for the performance of its tasks.

On the other hand they might issue warnings to a controller or processor that intended processing operations are likely to infringe provisions of the GDPR or impose an administrative fine, in addition to, or instead of other measures referred to in the GDPR, depending on the circumstances of each individual case.

Pursuant to Art. 56 (6) GDPR one Lead Supervisory Authority shall act as a sole contact point for the controller or the processor whose processing activities affect multiple EU member states which often will be the case. So, by choosing the seat of the main establishment of a company it also automatically chooses the lead authority. Depending on how strict a national authority is this might be a choice of impact. In any case, please notice that this “One-Stop-Shop” procedure will not apply where certain data processing activities are solely performed in one particular branch or establishment of a company in one country. In this case, the authority in this one particular country remains competent.

■ **Checklist**

- Always ensure that you comply to the obligation to cooperate with the supervisory authority by designating one person in charge for communicating with the supervisory authority
- In case of transnational dimension: identify which Supervisory Authority shall be your single contact point.
- Train and implement mechanism to make sure those tasks are carried out effectively.

11 Data Breaches – What happens if a breach occurs?

A personal data breach occurs when personal data is illegally or accidentally:

- Destroyed or lost (e.g. deletion of personnel file, damage to a data medium, theft of a laptop, loss of a business mobile phone);
- Changed (e.g. adapting master data, accidental deletion of specific data fields, damage to a file); or
- Disclosed (e.g. misdirected e-mail, accidental activation of remote access, unauthorized access to an employee's personnel file).

As a general rule, the competent EU data protection supervisory authority is to be informed about the incident within 72 hours. The obligation lies with the controller.

The notification shall describe

- (i) the nature of the personal data breach including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned;
- (ii) communicate the name and contact details of the data protection officer or other contact point where more information can be obtained;
- (iii) describe the likely consequences of the personal data breach; and
- (iv) describe the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.



Processors have to ensure that controllers are properly noticed without undue delay of any such activities to enable them to comply with their obligations (see Art. 33 GDPR).

Note: The period of 72 hours is not extended when the incident happens on the weekend or a holiday. So, whenever you detect a breach time is of the essence!

In cases where the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, e.g. where imminent damages are to be expected for the data subjects, the controller shall communicate the personal data breach to the data subject without undue delay. Avoiding such a notification is usually in the interest of any concerned company but depending on the scope of the breach sometimes hard to manage. In any case, the notification would need to be issued without undue delay as well.

If you notice or suspect a personal data breach, the responsible stakeholders must immediately be informed to take any measures necessary. To guarantee the proper dealing with such scenarios a company needs to establish effective procedures, define responsibilities and properly document it.

Depending on how well the response team is able to react and minimize any damage during such a data breach incident will have a huge impact on how much your company is then fined and / or penalized.

To deal with data breaches properly the following checklist might be of help:

■ Checklist

- Response Plan: set up a sufficient reporting procedure in case of data breaches which includes rules on who is responsible, who has to inform whom and when a breach is a reportable data breach.
- Train your employees accordingly.
- Test if plans and mechanism work in order to being prepared.
- Know where you reach your competent authorities in case you need to report!

12 GDPR Compliance – Can I certify that?

Data protection authorities are rather reluctant to accept available certifications that are common in the IT sector for certifying companies IT-security concepts as a sufficient proof for GDPR compliance.

However, more and more companies wish to rely on standards and certifications in order to proof their compliance with legal requirements. The GDPR lawmaker recognized this development as GDPR now outlines in Articles 40 and 42 (1) GDPR, that codes of conduct and respective certification mechanisms shall be established “for the purpose of demonstrating compliance with” the GDPR by controllers and processors.

As you can see from the law, being certified does not prove compliance in and of itself but rather constitutes a way to demonstrate compliance. However, up until now, there are no approved codes of conducts or certification schemes or accredited certification bodies for issuing GDPR certificates as indicated by the GDPR.

There are of course certain standards and best practices that are - more or less - endorsed by regulators in the EU to proof GDPR compliance or at least for parts of it, Certification according to ISO 27001 would be a well known approach to certify at least parts of the compliance requirements set by e.g. Art. 32 GDPR, Besides there are a number of GDPR and IT security related schemes that are regularly used in business practice, while GDPR certification schemes according to Art. 40 GDPR are still to be awaited,

Closely monitor current developments to be well-informed on what regulators endorse as GDPR certifications - once available - will,



V Typical Use Cases

In the following, we would like to present typical use cases, where it is inevitable to take measures in order to comply with the GDPR. You will most likely see yourself in at least one or two of the following scenarios regardless of the size of your company and the industry you are part of.

1 GDPR and operating a website or an app

Nearly every entity has an online presence - be it in the form of a website, a social media page and / or an app. And you guessed it right: (almost) all of them are subject to the GDPR, at least when you are targeting natural persons within the European Union (see for the territorial scope Section 2 above). This means, when operating a website that is also addressed to a European audience - notwithstanding if local language is provided or not - GDPR will usually apply. Please also note that targeting European website users with tracking technology (e.g. tracking cookies or retargeting / advertisement networks) or by collecting log-files such as IP addresses or other personal identifiers (e.g. the MAC address of a device) may trigger the applicability of the GDPR.

Getting your online presence - for most the face of the company and main platform for communicating with customers - up to par will make a huge impact on your overall GDPR compliance.

Having a sound privacy policy in place will be a first and indispensable step. In order to fulfil your extensive information obligations (see 3.1), you will first have to review and evaluate your website / app to determine the functions that are relevant to data protection. Be sure to understand what they are doing so you can inform the user accordingly.

Besides providing for a proper policy you need to assess whether the way you collect and process personal data is legit. Some of the most common functions you would apply on your website are:

1. Tracking tools (e.g. Google analytics)
2. Registration forms
3. Newsletter sign-up forms
4. Cookies
5. Social media buttons
6. Contact forms
7. Payment gateways on e-commerce websites (e.g. Paypal)

Please note that you need to have a legal basis for each of the processing activities. When offering a website these usually narrow down to “contract performance” (Art. 6 (1) b GDPR, e.g. for answering an e-mail request) or “legitimate interest” (Art. 6 (1) f GDPR, e.g. for applying technical safeguards or conducting certain marketing activities).

■ Please note:

If use profiles (tracking) are created to evaluate the use of websites and apps, the data subjects must always be informed accordingly in the privacy policy statement.

Personal tracking may only be carried out if it is permitted under national law or upon consent of the data subject. In this course European regulators tend to become very strict lately and require consent for a lot of activities. Notwithstanding the overall legitimacy of a procedure (e.g. do we separate consent or not) the data subject should always be given the chance to opt out from a tracking and marketing activities in an easy and transparent way.

If websites or apps can access personal data in an area restricted to registered users, the identification and authentication of the data subject must offer sufficient protection during access.

Also, consider increasing your website security. You need to make sure to take measures to fully protect the personal data you have processed. Possible security measures include:

- encryption
- use a secure host (check hosting company' s security plan and security level)
- constantly maintain your website and keep your software up to date
- practice strict access control and password policy
- have a reliable backup routine in place
- regularly perform security checks

These are just a view measure to take to work towards website compliance. However, for starters the following points would need to be checked thoroughly and sum up the most relevant requirements:

■ Checklist

- ✓ Identify data protection relevant functions within your website, app or webservice
- ✓ Make sure that there is a proper legal basis for each purpose or function
- ✓ Check if all of them are necessary and / or if you can substitute them for data protection friendlier alternatives
- ✓ Tracking and online marketing are quite complex in Europe from a data protection perspective - things are in transition at the moment. Check whether the tools you wish to use or the procedures you plan require separate consent and how it should be implemented.
- ✓ Draft or amend your privacy policy accordingly - it's the key for any GDPR website concept! And remember: it is always safer to give more than less information
- ✓ Check your security plan and act accordingly!

2 Employee data - is there anything different?

Even if you are a small sized company, you will surely collect and use personal data belonging to job applicants, employees or workers. When your employees are located in Europe (e.g. with one of your company groups entities) you will most certainly be required to comply with the requirements of the GDPR when processing their personal data. The rules set out so far in this handbook will apply with no exemption. Further, certain processing activities that are quite common when processing employee data might require additional steps you should know about.

In short: Employers are obliged to protect their employees' data from the initiation, throughout the execution and even after the termination of the employment relationship.

■ Examples

- Initiation phase: collection of employee data when recruiting employees by requesting or receiving personal data in job application forms and CVs.
- During employment: processing of data in relation to salary and benefits entitlements, performance reviews and disciplinarys and grievances.
- After termination: legal obligation to retain data for certain periods of time (e.g. tax regulations, statutory sick pay payments etc.).

Keep in mind: When processing data of your employees you must have a lawful reason for it and ensure it is done fairly, only for a limited period of time and kept accurate and secure!

During the course of employment, further relevant processing activities might be carried out: personal data of employees might be collected for security purposes to ensure the integrity of the companies IT-systems (e.g. system log files). Where the compound is fixed with CCTV, cameras will also record employees, which requires a very thorough evaluation of the legal requirements. Also, when administrating sick leave sensitive categories of data might be collected and processed (e.g. health data) and will, thus, have to be treated with particular care and diligence.

It will be very challenging to base any such processing activities on the employee's consent within the scope of the employment, as consent needs to be given by free will and its validity is often questioned in the employmentship. Therefore, proceed with care when using consent to obtain a legitimate basis for the processing of personal data as in most of the cases it will not provide for a practical legal basis.



In any event, having an *employee data protection policy* in place is vital. It can significantly reduce the risk of claims for failing to comply with applicable laws. Such a policy should list all relevant processing purposes, the collected personal data, by whom the data will be processed and how employees can obtain further information on it and how to make use of their rights as data subjects. As you may often process personal employee data based on legitimate interests informing data subjects properly becomes even more important.

We could go on for pages and pages as employee data protection is a very complex topic. However, the following basic principles should provide for a good checklist for starters:

■ **Checklist**

- ✓ Remember that employees are also data subjects in the meaning of the GDPR!
- ✓ The GDPR rules you already learned apply to your employees as well – of course limited to cases where you are in scope of the GDPR which is either the case where you process personal data from European employees or where the processing activities with regards to employees (wherever they are located) are base in the EU.
- ✓ Check if you have a legal basis for every processing activity. If you base any processing activities on consent, make sure it is given by free will or even better, see if you can find another legal basis.
- ✓ Have an employee data protection policy in place! It helps to be aware of what you do with your employee data and also provides guidance and steers the processing of employee personal data a great deal. A good employee privacy policy will be a solid basis for employee data protection.
- ✓ Consider that several EU member states provide for deviating rules for employee data protection in their local data protection laws. This is permitted as the GDPR leaves room for these deviations. These make it quite hard for employers to design pan-European data protection law concepts. So m be aware that things might be different depending on where the activities are located. Do a local double check if necessary!

3 Marketing – what does GDPR permit?

Marketing and GDPR can be quite tricky. Marketing is an essential part of running a business or organisation and it is in its inherent nature to know or - based on current knowledge - anticipate the needs and wants of existing and potential customers. For that, personal data is of essence. On the other hand, GDPR has changed the way companies can communicate with customers. Because of the increased awareness among the public, customers no longer hold back and express their displeasure by lodging a complaint with the supervisory authorities if they feel bothered. So, be extra careful when using customer data for marketing purposes!

When looking at marketing and the legal framework applicable to it please consider that there are several laws in the EU governing these activities. Besides GDPR there are certain national laws regulating marketing activities by electronic means (e.g. by e-mail). In parallel, European lawmakers discuss a new “ePrivacy Regulation” covering especially online and media data use cases, which was supposed to come into force together with GDPR but is still pending.

However, according to specific laws in the EU member states (e.g. for Germany the Law against Unfair Competition) marketing purposes such as the sending of newsletters or other offers by e-mail or informing customers about it by phone usually requires explicit consent of the data subject for which rather strict formal requirements are to be observed. For this very narrow exemptions apply.

From a GDPR angle marketing measures might even be privileged as it is recognised within the GDPR recitals as a legitimate interest of a controller. But even according to GDPR not everything is possible without consent: specific forms of customer profiling, web tracking

or the use of special categories of personal data may require separate consent.

In any event, if a customer withdraws its consent to receive marketing information this has to be strictly observed. Businesses must not conduct direct marketing activities if a customer does not want it.

To follow the accountability principle, especially for marketing via e-mails a **double opt-in** procedure is recommended in order to obtain a provable consent. This means that the advertiser sends an e-mail to the customer or partner who has given consent (e.g. when registering via a website) and asks for confirmation of such consent. Marketing should only be sent upon receipt of such a confirmation, which should always be stored and documented properly. Once consent has been given, the respective customer or partner may be contacted for marketing purposes in which he has consented without further explicit consent as long as the recipients do not object (so called “opt-out”).

Since, as described above, this is a field where customer disputes regularly occur, we urge you to take every single customer request seriously and react to it promptly and diligently. The following checklist may help to implement a proper concept:

■ Checklist

- ☑ Go through all of your marketing activities and check if you have the necessary consent or other legal basis if required.
- ☑ Make sure that consent - if necessary - is obtained the 'right way' (e.g. opt-in, no pre-checked boxes,...)
- ☑ Inform data subjects on how you use their data related to marketing (e.g. in your privacy policy).
- ☑ Consider that certain processing activities may require additional steps, e.g. when related to profiling or targeting.
- ☑ Have a reliable response plan in place: react promptly to any customer requests! Otherwise, you risk that the customer lodges a complaint with the supervisory authority.

4 Big Data

Big Data is not only a very popular way of making use of huge loads of data to better understand your business and to draw interesting conclusions from available data. It also imposes a few struggles on those performing it because certain restraints GDPR provides.

Firstly, when you perform Big Data assume that almost any data you use for it will be personal data. The bigger the load of data is you use for your analysis the higher the chance that by connecting certain data it might allow you to re-identify a natural person behind it. So, first and foremost aim when performing Big Data is to use anonymized data for it. For better understanding how to achieve that please refer to Section 2.1 above. Anyways, regard proper anonymization of data sets for Big Data as a very challenging exercise. Unless you are really sure you can achieve it, get used complying with GDPR!

The principles you have to regard are the same as always - please refer to the above parts of this handbook. However, let's look at the following three (3) typical issues that usually come up with Big Data and GDPR:

Firstly, you recall that you have to inform data subjects on how you treat their personal data (Art. 13, 14 GDPR; see above). However, typically companies decide to use personal data for Big Data way after it has been collected which then constitutes a change of processing purposes (Art. 6 (4) GDPR). By law, you would then have to inform the data subject on your plans in a transparent manner which may require you to go back to the data subject and tell them (e.g. with a revised privacy policy).

Secondly, as we now learned that using data for Big Data purposes usually leads to a change of processing purposes (see Art. 6 (4) GDPR), you need to determine another legal basis for this particular purpose. Sometimes, you might be able to base such a processing on legitimate interests (Art. 6 (1) f) GDPR). Depending on the actual circumstances, e.g. the way you use data, the level of risk for re-identification of the data subject and the category of data and its sensitivity, Big Data use might, however, require other means to be legit, for example separate consent of the data subject.

Thirdly, Big Data projects sometime come with the involvement of a data processor (e.g. a service provider) with access to the data. As you recall, involving a processor requires a Data Processing Agreement according to Art. 28 GDPR and further safeguards. So, don't forget to take care of these before granting access to the data for the service provider.

So, to summarize it you can see that defining your intended purposes prior to collecting and processing personal data is of great value. Privacy by design is a major concept to consider for implementing the right steps at the right time.

5 Internet of Things

Another fashion that brings a load of implications with GDPR would be the Internet of Things ("IoT"). Whether you sell devices or offer services that allow for a comprehensive connectivity and data transmissions that characterize IoT services, it will always include the collection and processing of data.

Firstly, it is important to understand if you deal personal or anonymized data. For example, if you offer services that help a customer to control connected devices in a smart home environment the data collected will usually include a reference to the owner of the device or the property - may it be a customer ID, IP address or other identifier. So, again we see that achieving anonymization is harder than it seems.

As always, you need a legal basis to process data collected through IoT services or devices. If related to performing a contract Art. 6 (1) b) GDPR may apply in your favour. However, sometimes you may decide to use the collected data for other purposes such as product development, predictive maintenance services or upselling and marketing activities. For these purposes legitimate interests (Art. 6 (1) f) GDPR might help but - again - certainly not in all of the cases. In this context please consider that especially IoT devices and services may trigger certain risks for the data subjects which may originate from profiling, automated decision making or other sensitive data processing activities, e.g. when processing special categories of personal data. These will have a great impact on the balancing test when basing a processing on a legitimate interest. So - long story short - find a proper legal basis for each and any purpose you wish to follow when using data from IoT devices and services before you start.

If you come to the conclusion that you might need to obtain consent for the processing you intend you might face another obstacle. Depending on your role as to the processing of personal data - controller or processor - or your relation to the data subject (Is it yours or another company's customer?) consent might sometimes be hard to obtain for you. The same struggles you may face when you have to inform the data subjects according to Art. 13, 14 GDPR.

Especially when the data subject has no direct relationship with you this might be difficult to handle, as IoT devices often do not provide for proper mechanisms to display data protection law related information unless you are operating it together with an app or webservice. As but not least, as IoT devices and services tend to collect a vast amount of data it is always a challenge to get rid of it afterwards. So, when collecting data in this context always consider the principle of data minimization and think of a way on how to properly store and erase data afterwards.

6 Healthcare services and GDPR

As we have already learned, GDPR requires more caution when processing special categories of personal data, especially when relating to an individual's health. The GDPR regulates the use of "genetic" and "biometric" data. So, it is clearly visible that processing personal data in the health sector is specifically regulated by GDPR and imposes stricter requirements on a controller (and a processor for that matter) than when dealing with other types of data.

As a general principle, personal health data may only be processed with the express consent of the data subject. One solution - as always - might be to anonymize data before processing it. Again, this will work in very narrow cases only, but will always be the “Gold Standard” if you can achieve to. Although regulators are yet to provide specific guidance and standards in relation to the threshold of anonymization it is already fair to say that the bar will be set very high as the risks connected to processing health data are as well.

The above does not mean that processing health data will always require a consent. GDPR does allow for the processing of health data on the basis that this is required for the performance of a contractual obligation, such as the delivery of a health related service, e.g. when you run a hospital. However, the line to draw is very thin and the interpretation of what is needed to perform the contract is strict and to a certain extent defined by law (see Art. 9 (2) GDPR and related national laws, e.g. in the sector of employee data protection).

Certain processing activities may fall outside of this scope, e.g. when profiles which have been created from the user's health data are used for purposes other than those the data was originally requested for (e.g. a patient's medical treatment). In these cases, obtaining consent will likely be required.

Transferring personal health data to third parties (e.g. a technical service provider) usually requires very strict safeguards. Obtaining consent might be advisable as to the sensitivity of the processing activities and given the general rule in the GDPR (see Art. 9 GDPR). However, lately there has been a certain liberation for these types of services so that consent might not be required for any transmission and processing by third parties.

However, as the disclosure of e.g. patient data is still strongly regulated under criminal laws in several EU member states (which apply in parallel to the GDPR) a thorough assessment



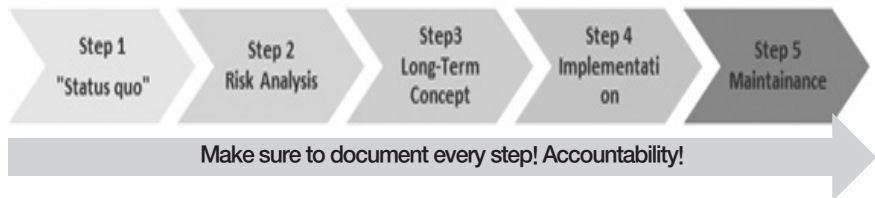
of your planned data processing activities is highly recommended. If you offer these types of services strict technical and organisational measures (Art. 32 GDPR) will be a key component to achieve GDPR compliance.

Again, a specific focus should be placed on “Privacy by Design” and “Privacy by Default” as these require companies already in the development stage to ensure that services are structured and developed in a way that it collects as little data as possible.

VI Step-by-Step Guide

After working through this handbook working your organization towards a GDPR compliant setup might seem like a daunting task as the vast amount of provisions and the flood of new information can be quite overwhelming. But the most important thing is to get started and take action,

We recommend the following approach:



Step 1: Analyse your current situation using the checklists provided

- Allocate resources and budget to cover the project - it might be a long way!
- Appoint a GDPR core team and one responsible person for each department
- Get management attention - the risks GDPR imposes should be enough to create awareness!
- Clarify the following points:
 - What kinds of personal data do you process?
 - What are your processing activities?
 - Why - for what purpose - do you process them?
 - Where, how and for how long to you store them?

- Who has access to them?
- What are the legal bases?

Step 2: Analyse the potential (high) risks

- Analyse audit the findings of all departments, in particular with regards to the procedures that seem to bear the highest risks
- Set priority list accordingly
- Address the most risky concerns first
- Apply first wave remedies (i.e. privacy policies, data processing agreements, consent forms···)

Step 3: Develop a long-term concept

- Allocate resources and budget accordingly after you have a first understanding of what is to come
- Designate a person in charge to implement GDPR safeguards and oversee the procedure (either own personnel or an external advisor)
- See GDPR as a chance (streamline your volume of data, increase efficiency of processes, part with outdated systems, upgrade to new more efficient and safe technologies)

Step 4: Implementation

- Implement necessary measures step by step
- Prioritize sensitive procedures over less critical ones
- Going live - Make sure to act in concert
- Raise awareness through workshops and trainings

Step 5: Maintenance

- Constantly check if mechanisms operate reliably
- Adapt procedures where necessary
- Keep an eye on newest developments in technology, EU and national legislations and decisions of the supervisory authorities (i.e. enforcement of penalties)

VII Sources for further information and instructions on GDPR

As this Handbook can only give you a limited overview on the most relevant aspects of the GDPR you may wish for further and more detailed guidelines and materials on GDPR after you have worked through these first aid guidelines.

We can recommend to start at the website of the European Data Protection Board (formerly known as “Article 29 Working Party”) that publishes guidelines on how to interpret and apply GDPR. These will help you to get a better understanding of the legal framework and provide many helpful examples on how to apply it to your daily business.

(*edpb.europa.eu/edpb_en

Selected guidelines which will be a great help to further work yourself into GDPR compliance can be downloaded in particular under the following links:

| | |
|--|---|
| Guidelines 3/2018 on the territorial scope of the GDPR (Article 3) | https://edpb.europa.eu/sites/edpb/files/consultation/edpb_guidelines_3_2018_territorial_scope_en.pdf |
| Guidelines on consent (WP259rev,01) | https://ec.europa.eu/newsroom/article29/item-detail_cfm?item_id=623051 |
| Guidelines on transparency (WP260rev,01) | https://ec.europa.eu/newsroom/article29/item-detail_cfm?item_id=622227 |
| Guidelines on Automated individual decision-making and Profiling (WP251rev,01) | https://ec.europa.eu/newsroom/article29/item-detail_cfm?item_id=612053 |
| Guidelines on personal data breach notifications (WP250rev,01) | https://ec.europa.eu/newsroom/article29/item-detail_cfm?item_id=612052 |

| | |
|---|---|
| Guidelines on the right to data portability (WP242rev.01) | https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611233 |
| Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is “likely to result in a high risk” (WP248rev.01) | https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611236 |
| Guidelines on Data Protection Officers (DPO) (WP243rev.01) | https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612048 |
| Guidelines for identifying a controller or processor’s lead supervisory authority (WP244rev.01) | https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611235 |
| Position paper on the derogations from the obligation to maintain records of processing activities pursuant to Article 30 (5) GDPR | https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=624045 |
| Working document setting forth a co-operation procedure for the approval of “Binding Corporate Rules” for controllers and processors under the GDPR (WP263rev.01) | https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=623056 |
| Recommendation on the standard application for Approval of Controller Binding Corporate Rules for the transfer of personal data (WP264) | https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=623850 |
| Adequacy Referential (WP254rev.01) | https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=614108 |
| Guidelines on the application and setting of administrative fines (WP253) | https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611237 |

The above listing is only an excerpt of the available guidelines. Please see the website for further documents.

In addition you will find further guidance on international data transfer based on the so-called EU Standard Contractual Clauses on the websites of the European Commission(*) under including the current sample documents for international data transfer.

Last but not least, France, Germany etc. several national data protection authorities provide

guidance for companies to check out with regards to specific topics including how to draw up a proper data processing agreement. (**)

Lastly, several interest groups such as BITKOM e.V.(***) in Germany provide helpful guidance for free on the internet.

(*) ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/model-contracts-transfer-personal-data-third-countries_en

(**) edpb.europa.eu/about-edpb/board/members_en / (France) www.cnil.fr / (Germany) datenschutz-wiki.de/Aufsichtsbeh%C3%B6rden_und_Landesdatenschutzbeauftragte

(***) bitkom.org/EN

Writers of this handbook is a team of GDPR Specialists from international law firm Taylor Wessing :



Thomas Kahl
Salary Partner
Data Protection Specialist
Frankfurt am Main /
Germany
t.kahl@taylorwessing.com
+49 (0) 69 97130 111
Dr. Julia Wulf



Dr. Julia Wulf
Partner
Data Protection Specialist
Frankfurt am Main /
Germany
j.wulf@taylorwessing.com
+49 (0) 69 97130 0



Dajin Lie
Associate
Korean Desk
Frankfurt am Main /
Germany
d.lie@taylorwessing.com
+49 (0) 69 97130 111

작 성 자 TaylorWessing

번역감수 KISA 한국인터넷진흥원

EU 진출 기업을 위한
유럽 일반 개인정보 보호규정(GDPR) 핸드북

발행인 권평오
발행처 KOTRA
발행일 2019년 7월
주 소 서울시 서초구 헌릉로 13
전 화 1600-7119(대표)
홈페이지 www.kotra.or.kr
I S B N 979-11-6490-010-7 (93320)
979-11-6490-011-4 (95320) (PDF)



Copyright © 2019 by KOTRA, All rights reserved.

이 책의 저작권은 KOTRA에 있습니다.

작 성 자 TaylorWessing

번역감수 KISA 한국인터넷진흥원

kotra

대한무역투자진흥공사