# GDPR 컴플라이언스 위한 가장 시급한 일 6 가지

**GDPR, 기업의 데이터 관련 행태 체질부터 바꾸라 요구**
**정책 변경하고 옵트 인 방식 활용하고 불필요 데이터 지우고**

[보안뉴스 문가용 기자] 지금부터 한 달 뒤인 5 월 25 일에는 유럽연합의 새로운 개인정보보호법인 GDPR 이 시행된다. 이제 유럽이라는 땅 덩어리 내의 모든 사이버 프라이버시 관련 규칙은 이 GDPR 을 기준으로 만들어질 것이다. 만약 당신의 사업이 유럽인들의 개인정보를 필요로 한다면, GDPR 을 반드시 염두에 두어야 할 것이다.

기억해야 할 것은 GDPR 이 데이터 보안 관련 법이 아니라 프라이버시와 관련되어 있다는 것. 물론 둘이 완전 별개의 것은 아니지만, 동일한 것도 아니다. 그렇다면 GDPR 을 준수하려면 구체적으로 뭘 어떻게 해야 하는 걸까? 방대한 GDPR 문건과 가이드라인 앞에 넋이 빠져버린 당신을 위해 여섯 가지 절차를 요약해본다. 물론 이 순서가 절대적이거나 모두가 동의하는 건 아니다.

1) 일반 대중들에게 노출되는 프라이버시 관련 정책을 변경하라. 프라이버시 정책은 GDPR 규제 기관이 가장 먼저 요구하고 확인하는 공식 문건이고, 당신 기업의 얼굴이다. 정책부터 GDPR 과 맞지 않는다면, 더 들여다볼 것도 없이 위반이다. 또한 여기서부터 틀리면 GDPR 규제 기관이 더 꼼꼼하고 빡빡하게 점검을 시작할 것이다.

2) 데이터가 실제 어디에 위치해 있는지를 정확히 알고 있으라. GDPR 은 결국 유럽인들의 개인식별정보를 어떻게 관리해야 하는지에 관한 규정이다. 이는 즉 그러한 민감 정보가 정확히 어디에 있는지, 기업이 얼마나 보관하고 있는지, 어떤 방식으로 보호되고 있는지, 누가 어떤 절차로 접근하는지를 알아야 한다는 소리다.

그런데 문제는 이 '위치 파악'이 말처럼 쉽지 않다는 것이다. 데이터의 흐름을 매핑한다는 건 대단히 큰 규모의 작업이다. 그런데 GDPR 체제 아래서는 꼭 해야만 한다. 만약 백업을 꼼꼼하게 하는 기업이라면, 오히려 수많은 하드드라이브에 개인식별정보가 널려 있을 수 있다. 그래서 전문가들에 따라서는 '데이터 매핑' 작업이 5 월 25 일 이전에 끝낼 수 없다고도 한다.

3) 프라이버시 보호 정책을 시행하고 지키는 걸 습관화 및 문화화 하라. 유럽연합의 영토 내에서는 기업의 의도가 법의 정확한 명문보다 우선시 될 때가 많다. 즉 개인식별정보를

보호하고 유출을 막고자 한 올바른 정책과 기술, 절차를 가지고 있고, 그걸 따르고자 하는 의도를 충분히 가지고 있는 것이 무엇보다 중요하다는 것이다.

4) 그 다음은 데이터 보호 책임자인 DPO 를 고용하는 것이다. 그런데 사실 모든 회사가 전부 DPO 를 필요로 하는 건 아니다. 커피샵을 유럽에서 운영한다면, DPO 가 필요하지 않을 가능성이 높다. 하지만 유럽시민의 개인정보를 수집하고 분석하는 일을 수행해야만 되는 사업을 운영한다면 DPO 가 필요할 것이다.

그러나 현재 DPO 찾기란 매우 어려운 일이라고 알려져 있다. 하지만 이들을 찾을 수 있는 경로는 크게 세 가지로 좁혀진다. 외부 인재를 영입하거나, 내부 직원을 DPO 로 육성하거나, DPO 서비스를 외주 업체에게 주는 것이다. 의외로 가능성들이 하나 둘 열리고 있으니, 처음부터 너무 완벽한 인재만을 바라지 않아도 될 것으로 보인다.

5) 데이터 수집 절차를 '옵트 인'으로 바꿔야 한다. 즉 수집 대상이 원할 때만 정보 수집이 이뤄지도록 해야 한다는 것이다. 현재 대부분 기업들은 사용자의 정보를 요구할 때 '옵트 아웃' 방식을 활용한다. 수집하고 있다가 사용자가 원하지 않는다고 요청을 해야만 수집을 멈추는 방식이다. GDPR 은 절대적으로 옵트 인 방식만을 지지한다. 수집 행위가 일어나기 전에 동의를 받아야 한다는 것이다.

여기에 더해 옵트 인을 해야만 서비스나 앱을 사용할 수 있도록 하는 업체들의 약관 행위도 GDPR 은 허하지 않는다. 원하지 않는다 혹은 허용하지 않겠다는 소비자들도 해당 서비스나 앱을 사용할 수 있어야 한다고 GDPR 은 규정하고 있으니 개인정보와 관련된 '꼼수'는 더 이상 부리지 말아야 한다.

6) 필요하지 않은 건 삭제하라. 대부분 기업들이 최대한 모으고 최대한 오래 저장하는 것을 습관처럼 행하고 있다. 그 정보가 필요하든 필요치 않든 상관없이 말이다. 그러나 이제는 이러한 행위에 커다란 책임이 따라붙게 되었다. 이제 어떤 사람의 정보를 가지고 있으려면 그 사람 개인의 허락을 얻어야만 한다.

그러므로 유럽인에 대한 정보를 사업적으로 불필요하게 가지고 있다면 삭제하라. 어디에 따로 백업해두지도 말라. 누군가 데이터를 유출시켰을 때 이런 불필요한 개인정보마저 유출되면, 피해가 두 배 세 배로 커진다.

[국제부 문가용 기자(globoan@boannews.com)]