Yulchon Legal Update

2025.04.

인도네시아 개인정보 보호법(Personal Data Protection Law, PDPL)의 본격 시행 및 기업의 실무 리스크 점검 및 대응 전략

1. 인도네시아 개인정보보호법(PDPL) 개요

인도네시아는 오랜 기간 개인정보 보호에 관하여는, 기본 법령을 제정하지 아니한 채, 개별 부처별 규정에 의존해 왔습니다. 그러나 최근 디지털 산업의 성장과 함께 온라인상 주요 기업의 개인정보 유출 사고가 빈번히 발생하였고, 그로 인하여 국민의 개인정보 보호에 대한 요구와 국제사회 기준에 부합하는 입법 필요성이 커졌습니다.

이에, 인도네시아는 2022년 10월 「2022년 제27호 개인정보보호법(PDPL)」(이하 "PDPL")을 제정하여, 동남아 주요국 중 다섯 번째로 종합적인 개인정보보호 법령을 입법하였습니다. 동 법은 2년간의 유예기간을 거쳐 **2024년 10월 17일부터 전면 시행**되고 있으며, 그에 따라 인도네시아에서 개인정보를 수집·이용하는 모든 기업은 PDPL을 준수해야 합니다.

대다수 국가의 개인정보 보호 법령과 유사하게, 인도네시아의 PDPL 또한, 유럽연합의 General Data Protection Regulation (GDPR)의 입법 구조를 상당 부분 반영하고 있고, 개인정보 보호 법령의 핵심적인 내용이라고 할 수 있는 개인정보의 정의, 정보주체의 제반 권리, 개인정보처리자의 개인정보 보호의무, 감독기관의 권한, 행정·형사 제재 조항을 모두 포함하고 있습니다.

2. PDPL의 주요 내용

가. 역외적용 조항

PDPL은 인도네시아 공화국의 법적 영역 내에서뿐만 아니라 인도네시아 국민인 정보주체에게 법적 영향을 미치는 경우 적용된다는 취지의, 소외 '역외적용 조항'을 두고 있습니다(PDPL 제2조). 따라서, PDPL은 인도네시아 내에서 활동하는 기업은 물론, **인도네시아 국민의 개인정보를 처리하는 모든 외국기업**에도 동일하게 적용됩니다(PDPL 제2조). 즉, 국내 본사에서 인도네시아 소비자의 정보를 수집하거나, 인도네시아 고객 데이터를 클라우드로 전송하여 처리하는 경우 등도 규제 대상이 됩니다.

Related Areas

인도네시아

Contact

이명재 외국변호사
02-528-5035
mjlee@yulchon.com

이태혁 외국변호사
02-528-5512
thyi@yulchon.com

최동찬 변호사
02-528-5468
dcchoi@yulchon.com

나. 개인정보의 정의 및 개인정보의 처리

(1) 개인정보의 정의 및 분류

PDPL은 개인정보를 **그 자체 또는 다른 정보와 결합해 개인을 식별할 수 있는 모든 정보**로 규정하며, 이는 전자적/비전자적 형식을 모두 포함합니다. 또한 민감정보로서 건강정보, 생체정보, 유전정보, 범죄기록 정보, 직계비속에 관한 정보, 기타 개인 재무정보등은 **추가적인 보호 조치**가 요구됩니다(PDPL 제1조, 제4조). 다만 일반 정보와 민감 정보의 구체적 취급 차이에 대해서는 법률 단계에서 명시되지 않아 향후 시행령 등을 통해 보완될 것으로 보입니다.

(2) 개인정보 통제자(Data Controller)와 개인정보 처리자(Data Processor)

PDPL은 GDPR과 동일하게 **개인정보 통제자(Data Controller)**와 **개인정보 처리자(Data Processor)**의 개념을 정하고 있는 바, 각 개념은 상호 다음과 같이 구별됩니다:

(ⅰ) **개인정보 통제자(Data Controller):** 개인정보 통제자는, 단독으로 또는 다른 통제자와 공동으로 개인정보 처리 목적을 결정하고 그 **처리에 대한 통제권을 행사하는 개인, 법인, 공공기관 등을 의미**합니다. 즉, **개인정보의 종국적인 처리 방향과 책임을 지는 관리 주체**로서, 한국 개인정보 보호법의 '개인정보처리자'에 유사한 개념입니다. 복수의 개인정보 통제자가 공동으로 개인정보를 처리하는 경우 상호 간에 목적과 책임을 명확히 합의해야 합니다.

(ⅱ) **개인정보 처리자(Data Processor):** 개인정보 처리자는, 개인정보 통제자의 지휘나 대리를 받아 개인정보를 처리하는 **개인, 법인, 공공기관 등**으로서, **개인정보 통제자의 지위를 위임받거나 개인정보 통제자를 대리하여 실질적으로 개인정보를 처리하는 자**를 말합니다. 개인정보 처리자는, 오직 개인정보 통제자의 지시에 따라서만 개인정보 처리 업무를 수행하게 되며, 따라서 개인정보 처리자기 독자적으로 개인정보의 처리 목적 및 수단을 결정할 수는 없습니다. 나아가, 개인정보 처리자는 개인정보 통제자의 수권 범위를 넘어서 개인정보를 이용하거나 제3자에게 제공하여서도 안 됩니다.

다. 정보주체의 권리

PDPL은 개인정보의 제공 당사자인 정보주체(Data Subject)에게 광범위한 권리를 부여하며, 개인정보 통제자는 이러한 **정보주체의 권리를 보장**할 법적 의무를 집니다. PDPL이 정하고 있는 정보주체의 주요 권리는 다음과 같습니다.

(ⅰ) **개인정보 처리에 관한 정보 제공을 받을 권리:** 개인정보를 요청하는 당사자의 신원, 법적 근거, 처리 목적 등에 대한 정보를 제공받을 권리입니다(PDPL 제5조).

(ⅱ) **접근권:** 정보주체가 자신의 개인정보 사본을 열람하거나 교부 받을 권리입니다(동법 제7조).

(ⅲ) **정정권**: 개인정보의 오류를 수정하거나 최신 정보로 업데이트할 권리입니다(동법 제6조).

(ⅳ) **개인정보의 처리 중단 및 삭제 요청권:** 자신의 개인정보 처리의 중단을 요구하거나, 불필요한 개인정보의 삭제 또는 파기를 요구할 권리입니다(동법 제8조).

(v) **처리 제한권:** 일정한 범위 내에서 자신의 개인정보 처리 제한을 요구할 권리입니다(동법 제11조).

(vi) **동의 철회권:** 개인정보 처리에 대한 동의를 철회할 권리입니다(동법 제9조).

(vii) **자동화된 처리에 대한 이의 제기권:** 전적으로 자동화된 처리에 의한 의사결정(프로파일링 포함)에 이의를 제기하고 인간의 개입을 요구할 권리입니다(동법 제10조).

(viii) **데이터 이동권(Data Portability):** 자신의 개인정보를 구조화되고 기계 판독이 가능한 일반적 형태로 제공받아 다른 통제자에게 이전할 수 있는 권리입니다(동법 제13조).

(ix) **손해배상 청구권:** 개인정보 처리와 관련한 위법행위로 손해를 입은 경우 손해배상을 청구할 권리입니다(동법 제12조).

위 각 권리들은 국가 안보, 법집행, 공익 등의 목적으로 일정 범위 예외가 인정될 수 있으며(동법 제15조 제1항), 정보주체는 권리 행사 요청 시 통제자에게 서면으로 신청해야 합니다(동법 제6조). PDPL은 폭넓은 정보주체의 권리를 규정함에 따라, 인도네시아 국민의 개인정보 자기결정권을 강화하는 한편, 기업들로 하여금 이에 대응하기 위한 절차 마련을 요구하고 있습니다.

라. 개인정보 보호의무

PDPL은 개인정보 처리 주체(즉, 개인정보 통제자 및 처리자)에 대하여 다양한 준수 의무를 부여하고 있는 바, 그 주요내용은 다음과 같습니다:

(i) **적법한 처리 근거 확보 및 동의 요건:** 개인정보 처리는 정보주체의 사전 동의를 원칙으로 하며, 동의는 명시적이고 구체적인 목적에 근거해야 하고 서면이나 전자적 형태로 기록되어야 합니다. 특히 법은 "명시적 동의"를 요구하여, 암묵적이거나 포괄적인 동의로는 부족하고 충분한 설명에 기반한 적극적 동의가 필요합니다. 즉, 정보주체의 사전 동의는 서면 또는 전자적 방식으로, 목적별로 구체적이어야 하며, 언제든지 철회 가능해야 합니다(PDPL 제20조).

(ii) **개인정보 처리 원칙 준수:** 개인정보 처리자는 목적 제한성, 처리의 공정성과 투명성, 정확성, 보존기간 제한, 무결성 및 기밀성 등 개인정보 보호 원칙을 준수해야 합니다. 예컨대, 개인정보는 명확한 목적 하에 필요한 범위에서만 수집·이용되어야 하며 정보주체에 처리 목적을 고지하고 동의를 받는 등 투명성을 확보해야 합니다. 또한 개인정보의 정확성을 유지하고 최신 상태로 관리하며, 보안 조치를 통해 무단 접근이나 누출을 방지해야 합니다. 위와 같은 원칙은 PDPL 조항 전반에 걸쳐 구체화되어 있습니다(동법 제16조 등).

(iii) **기술적·관리적 보안조치 의무:** 개인정보 처리 주체는 개인정보를 안전하게 관리하기 위한 적절한 기술적·관리적 보호조치를 시행해야 합니다. PDPL은 개인정보 보호를 위한 기술적 조치를 마련하고 위험 기반 접근법을 통해 보호 수준을 결정하도록 규정하고 있습니다(동법 제35조).

(iv) **개인정보 유출 통지 의무:** 해킹, 내부자 유출 등으로 개인정보 침해사고(무단 공개 포함)가 발생한 경우, 개인정보 통제자는 지체없이(72시간 이내에) 해당 사실을 개인정보 보호 감독기관(Data Protection Authority, DPA)과 정보주체에게 서면 통지해야 합니다(동법 제46조). 통지에는 유출된 개인정보의 범위, 발생 시점과 원인, 개인정보 처리 주체가 취한 대응조치 등이 포함되어야 합니다.

(v) **DPO(Data Protection Officer) 지정 의무:** PDPL은 일정한 조건 하에 개인정보 처리주체가 데이터 보호 책임자(DPO)를 지정하도록 요구합니다(동법 제56조). 구체적으로 공공 서비스를 위하여 개인정보를 처리하는 경우, 통제자의 주요 활동이 대규모 개인정보의 정기적·체계적 모니터링을 포함하는 경우, 통제자의 주요 활동이 민감한 개인정보나 범죄 관련 정보를 대규모 처리하는 경우에는 반드시 데이터 보호 담당자를 임명해야 합니다. 현재 PDPL은 DPO 자격 요건에 대해 "개인정보 보호 분야의 지식이 있는 전문가" 정도로만 규정하고 있어 추후 시행령에서 자격요건이나 임무에 대한 상세 기준이 나올 것으로 이해됩니다.

(vi) **보안조치 및 영향평가:** 개인정보 처리 주체는 기술적·관리적 보호조치를 마련해야 하며, 민감정보를 대규모 처리하거나 자동화 시스템을 사용하는 경우 사전 영향 평가가 요구됩니다(동법 제34조, 제35조). 이 또한, GDPR과 유사한 제도로서, 개인정보 처리로 인한 프라이버시 리스크를 사전에 식별·관리하기 위한 절차입니다.

(vii) **국외 이전 요건 준수:** 인도네시아에서 수집된 개인정보를 해외로 이전(국외 송출)할 때에는 개인정보를 제공받는 자가 소재한 국가의 개인정보 보호 수준이 인도네시아 PDPL과 동등하거나 더 높은 수준임을 보장해야 합니다. 구체적인 국외 이전 요건으로는, (i) 수신국의 개인정보 보호 수준이 동등하거나, (ii) 보호조치를 마련했거나, (iii) 정보주체가 명시적으로 동의한 경우에만 허용됩니다(동법 제56조).

마. 위반에 따른 제재

행정제재: PDPL을 위반할 경우 **행정적 제재와 형사 처벌**이 모두 부과될 수 있습니다. 우선 감독기관(DPA)은 법 위반에 대해 단계적인 **행정제재 권한**을 가지며, 위반의 정도에 따라 **시정조치 명령**부터 **과징금 부과**까지 다양한 제재를 할 수 있습니다. PDPL은 행정제재로서 (i) **서면 경고장 발부**, (ii) **일정 기간 개인정보 처리 활동의 정지 명령**, (iii) **위법하게 수집된 개인정보의 강제 삭제** 및 (iv) **과징금 부과** 등을 규정하고 있습니다. 특히 과징금의 경우 **위반자의 연간 매출 또는 이익의 최대 2% 한도**에서 부과될 수 있도록 정하고 있습니다. 다만 세부적인 과징금 부과기준이나 이의신청 절차 등은 법률에 구체적으로 명시되지 않았고, 향후 감독기관이 제정할 시행규칙에 위임된 상태입니다(동법 제57조).

형사제재: PDPL은 고의적이고 중대한 개인정보 침해행위에 대해 **형사처벌 조항**도 두고 있습니다. **타인의 개인정보를 불법적으로 수집·이용하거나 제3자에게 제공하여 자신이나 타인에게 이익을 얻고 정보주체에게 해를 끼친 경우**에는 최대 **5년 이하의 징역 또는 5억 루피아(IDR 500,000,000) 이하의 벌금**에 처해질 수 있습니다(동법 제67조 제1항). 또한 정당한 권한 없이 타인의 개인정보를 공개(누설)한 자는 최대 **4년 이하의 징역 또는 4억 루피아 (IDR 400,000,000) 이하의 벌금**에 처해집니다(동법 제67조 제2항). 한편 **허위의 개인정보를 만들거나 유포하여 자신이나 타인에게 이익을 얻거나 타인에게 해를 끼친 경우**(예: 존재하지 않는 정보로 타인을 가장하거나 조작하는 행위)에도 엄중히 처벌하며, 최대 **6년 이하의 징역과 6억 루피아(IDR 600,000,000) 이하의 벌금**이 부과될 수 있습니다(동법 제68조).

특히, PDPL을 위반한 주체가 법인의 경우, **영업정지 및 벌금형**의 대상이 되는 바, PDPL을 위반한 법인의 경우, **해당 범죄로 개인에게 부과되는 벌금액의 10배까지** 부과가 가능합니다. 그 밖에도, **범죄로 얻은 이익이나 자산의 몰수**, 관련 **영업허가 취소, 사업장 폐쇄, 법인 해산** 등 **추가적인 제재**가 부여될 수 있습니다. 아울러 법인 내에

서 실제로 행위를 한 **경영진, 책임자, 의사결정자** 등은 개인 자격으로 형사처벌을 받을 수 있어(예: 경영진에 대한 징역형) 관리자의 책임도 따르게 됩니다.

행정제재와 별도로, 정보주체는 민사상 손해배상 청구를 통해 피해 구제를 받을 수도 있습니다(동법 제12조).

3. 실무상 시사점 및 대응 방안

PDPL은 2022년 10월 공포 이후 기업들의 준비 기간을 고려하여 **최대 2년의 유예기간**을 거쳐 **2024년 10월 17일부로 본격 발효**되었습니다. 인도네시아 정부는 이 2년의 기간 동안 하위법령을 정비하고 감독기구 설립을 준비하는 한편, 기업들에 대해서도 법 준수를 위한 정비 시간을 부여하였습니다. 그 결과 대부분의 조항이 2024년 10월부터 효력을 가져 현재는 PDPL 규정이 전면 시행되고 있습니다.

이제 유예기간이 끝나고, 2025년부터는 본격적인 법 집행과 감독이 이루어질 전망이어서 인도네시아에서 활동하는 기업들도 이에 대한 대비가 시급합니다.

특히, 상당 기간 지연된 대통령 직속 개인정보 보호 감독기구(DPA)의 설립이 2025년 1분기 내 예정되어 있어, **엄격한 집행 국면**에 접어들 것으로 예상됩니다. 인도네시아에 진출한 또는 인도네시아인의 데이터를 처리하는 국내 기업들은 **동 법의 주요 내용과 최근 동향을 숙지**하고 내부 관리체계를 정비함으로써, 향후 발생할 수 있는 법적 리스크를 선제적으로 관리해야 할 것입니다.

다음은 국내 기업의 실무상 시사점 및 대응 방안입니다.

(1) 개인정보 처리활동의 PDPL 적용 가능성 점검

- 인도네시아 거주자나 국민의 개인정보를 수집하거나 보유한 적이 있는가?
- 현지 법인, 지점 또는 거래처를 통해 수집한 인도네시아인의 데이터를 본사 서버로 전송하는가?
- 현지 인력을 대상으로 HR, CRM, 마케팅 자료를 보관하고 있는가?

  → **위 항목 중 하나라도 해당되면 PDPL 적용 가능성이 높음**

(2) 관련 내규 및 절차 정비

- **동의서 및 개인정보 처리방침:** 목적별 고지, 철회 절차, 보유기간 명시 등 PDPL 기준 충족 필요
- **위탁 및 이전 계약:** 개인정보처리위탁 계약(Data Processing Agreement), 국외 이전 관련 표준계약서 등 PDPL에 맞게 개정 필요
- **DPO 및 대응체계:** DPO 지정, 정보주체 요청 대응 프로토콜, 유출시 대응 시나리오 마련

(3) 조직 내 교육 및 내부통제 강화

- 현지 법령 이해도 제고 및 현장 대응력 강화
- 개인정보 처리 단계별 리스크 및 통제 조치의 기록관리 및 문서화는 향후 조사 대응에 중요

(4) 법령 모니터링 및 현지 전문가 협업

- 향후 대통령령 및 시행령(PP) 제정에 따라 기업 의무가 구체화될 예정
- DPA 출범 후 가이드라인, 의무 신고 제도 등 새 규정 등장 가능

→ **현지 법률전문가와의 협업을 통해 선제적 대응 권장**

4. 마치며

PDPL은 인도네시아에서 이제 단순한 선언적 법률을 넘어, **실질적인 법적 집행이 시작되는 단계**에 접어들었습니다. 특히 인도네시아에 진출한 국내 기업은 자사의 글로벌 개인정보 처리구조를 고려하여, 인도네시아법과의 충돌 여부를 신중히 점검하고, 실무 대응책을 마련해야 합니다.

율촌 인도네시아 사무소는 고객사의 컴플라이언스 체계 수립과 대응 전략 마련을 위해 **현지 실무에 기반한 법률자문과 계약서·정책 정비를 지원**하고 있습니다. 필요 시 언제든지 문의 주시기 바랍니다.