アンラボ・セキュリティレター

Press Ahn

2018.10　Vol.58

オンライン個人情報処理ガイドライン、４年ぶりに改正

韓国オンライン個人情報処理ガイドライン改正

「オンライン個人情報処理ガイドライン」４年ぶりに改正

韓国放送通信委員会が 2018年9月18日「オンライン個人情報処理ガイドライン」を改正した。同ガイドラインはオンラインサービスの利用会員を対象に個人情報処理基準を提示することを目的とし、2014年11月に制定された。今回の改正ではユーザーが閲覧・提供を要求できる項目を事業者が持つ会員登録情報、事業者の利用状況、第三者に提供した状況などで具体化している。

今回のプレスアンでは、4年ぶりに改正された韓国オンライン個人情報処理ガイドラインについて紹介する。

今回の「オンライン個人情報処理ガイドライン」の主な改正点は大きく 6つに区分される。そのうち新規追加は 3つであり、既存の基準を現行化して情報主体の権利を強化させた事項が 3つだった。では重要度の高い「新規」事項から見てみよう。

1.個人情報の閲覧提供運用基準(新規)

■個人情報の閲覧/提供等対象項目及び方法の具体化

■個人情報の閲覧/提供等の要求に関する別途メニューの運用可能

■資料提供時に実費の範囲で手数料と配送料の請求可能

■閲覧提供の制限・拒否の理由を明示し、ユーザーに制限事由を通知

まず情報主体が、個人情報の閲覧提供を要求する項目を具体的に公開しなければならない。個人情報処理方針に必須閲覧提供項目を記載し、追加でホームページに別途メニューを作成して閲覧機能を提供しても良い。(個人情報処理方針は必要な処置で、サイトの別途メニュー作成は任意)

個人情報と自動生成された個人情報は、元々個人情報処理方針で公開する対象であったが、今回のガイドでは事業者が分析などを通じて生成した個人情報も含むように明示している。最近注目を集めているビッグデータ分析や、ユーザーのプロファイルを利用した購入傾向などの 2次個人情報がその例だ。

初回収集する場合や提供される場合は比較的ケースを識別することが容易だが、内部業務によって 2次生成される情報を把握することはかなり難儀が予想される。個人情報保護業務は通常のセキュリティチームやコンプライアンス管理チームが担当し、新たに発生する分析データまで継続して把握することが簡単ではない。個人情報保護業務を特定のチームで担当するよりも全社的なガバナンスとして対応すべき理由でもある。

個人情報の利用状況及び第三者への提供の公開も似たような負担がある。第三者への提供の場合、多くの企業が個人情報の処理方針に「第三者提供は、情報主体の同意がある場合や法令に基づく場合を除いて提供しない」などの原則のみ短く言及した場合が多い。しかし今回のガイドを順守するには、すべての組織で実際に発生した第三者への提供内容(プロバイダ、提供目的、提供アイテム、情報主体の同意又は法律の例外などの提供根拠)を記録してこそ閲覧要求に対応できる。これもまたそう簡単なものではなく、前述のように常時第三者への提供は、個人情報の処理方針に公開しなければならない。ここで言う第三者への提供は、一時的又は一回のみ発生する場合を意味する。

2. 個人情報処理方針の公開運用(新規)

■個人情報保護の業務処理部門、連絡先などの権利行使に必要な項目を、上段に明示するなどの処理方針の公開順序を変更する

個人情報処理方針の公開項目の順序が利用者の権利を中心に変更された。

[既存の公開順序]	[変更された公開順序]
1)個人情報の収集/利用目的、収集する個人情報の項目と収集方法	1)利用者及び代理人の権利と行使方法
2)第三者への提供の現状	2)個人情報保護の責任者の氏名と部門、連絡先
3)保有及び利用期間、破棄手順及び破棄方法	3)個人情報の自動収集装置の設置、運用、拒否事項
4)処理委託の現状	4)個人情報の収集、利用目的、収集する個人情報項目及び収集方法
5)利用者及び代理人の権利及び行使方法	5)第三者への提供の現状
6)個人情報の自動収集装置の設置、運用、拒否事項	6)保有及び利用期間、破棄手順及び破棄方法
7)個人情報保護の責任者、氏名、部門、連絡先	7)処理委託の現状

3. 利用履歴の通知運用基準(新規)

■個人情報利用履歴の個別/具体的な通知

情報主体の個人情報利用履歴を年1回以上定期的に報告する義務は、前年度末を基準に直前3ヶ月間、個人情報が保存・管理される利用者数が一日平均100万人以上か、前年の通信サービス部門の売上高が100億ウォン以上の事業者を対象とする。通知項目は、1)「個人情報の収集・利用目的及び収集した個人情報の項目」、2)「個人情報を提供された者と、その提供目的及び提供された個人情報の項目」、3)「個人情報の処理委託を受けた者、及びその処理委託をする業務の内容」にある。

従来は、個人情報収集の利用同意通知や個人情報処理方針の内容をコピーして貼り付ける程度の通知が一般的であった。今回のガイドでは第三者への提供の場合、個人情報処理方針に含まれていないか、あるいは同意の際になかった項目であっても実際に発生した提供内訳を各利用者に通知するように努めることを明示している。同項目で「通知しなければならない」と記載せずに「努める」と記したのは、これを実現するために相当な負担が伴うということに理解を示していることを表している。

例 : 個人情報利用履歴の通知

■個人情報の収集・利用目的及び収集した個人情報の項目

- 会員登録氏名、携帯電話番号、電子メールアドレス
- サービス利用及び相談 : 氏名、携帯電話番号、電子メールアドレス
- お支払い : クレジットカード社名、カード番号、有効期限、CVC
- キャンセル・払い戻し : 銀行名、口座番号
- 配送 : 受取人氏名、携帯電話番号、住所

■個人情報を提供された者と、その提供目的及び提供された個人情報項目

連番	1	2
サービス名	ooPay 利用会員	OO予約
提供を受ける者	(口座決済)OO銀行、 (クレジットカード決済)OOカード、 (携帯電話決済)COOテレコム ※提供した企業のリストをすべて記載	O社、O社、O社 ※提供した企業のリストすべて記載
目的	商品を購入及び配送サービス提供	予約プロセス、本人の意思確認、カスタマーサービス及び苦情処理
項目	ID、氏名、メールアドレス、電話番号、携帯電話番号、商品購入情報、受取人情報(氏名、住所、電話番号)	ID、氏名、電話番号、商品購入情報

4. 最小限の個人情報収集基準(現)

■本人確認がサービス提供に必ずしも必要ではない場合でも、個人情報を収集したなら「最小収集の原則」に反する

個人情報収集最小化の原則は、個人情報保護法の最上位原則である。「最小化」とは、主観的に判断される余地が多く、これまでは個人情報処理者が考える最低限の範囲と、情報主体が感じる最小限の範囲が異なる可能性が高かった。今回のガイドで提示した基準は、ある個人情報を選択したときにその情報がなくても情報主体がサービス利用に困らない場合、最小収集の原則に反すると判断される。例えば、静的なコンテンツのみで構成されるホームページで会員登録を強制する場合がこれに当たる。個人情報保護法が強化されて以来、このようなケースはあまり見られなくなった。

携帯電話や i-PIN[1]、公認認証書[2]などによる利用者の本人確認は、法律上の義務の履行やサービス提供に必須の場合を除き、利用者に強制してはならないとしている。利用者の本人確認が必要な場合でも、会員登録時ではなく実際のサービス利用時に本人確認をするように法律で定められていることを忘れてはならない。

14歳未満児童の個人情報収集に関しても留意内容がある。インターネット会員登録の段階で、満14歳未満の児童かどうかチェックするための具体的な措置を取らなければならない。生年月日を入力したり「14歳以上」という項目にチェックするなどの方法で、14歳未満の児童について明確に識別することをガイドは勧告する。

情報通信網法は主にオンライン会員に対する規制を含めているが、会員登録や個人情報収集の利用同意はオンラインのみ行われるものではない。オンラインサービスは初期から総括的な企画を通して構築され、設計段階で法的な準拠性を確認し、事前の処置をうまく実施するほうだ。だがオフラインは現場で作成した様式やフォームを使って業務が処理される場合が多く、IT部門やセキュリティ部門で把握しきれずにコントロールもできないため法令の基準に違反することが頻繁に発生しがちだ。

改正ガイドでは、オフライン上の個人情報収集について、以下のように様々なケース紹介を通じて適切な処置を提示している。

例① 本人確認と家族割引きなどの特典を提供するため、身分証明書(住民登録証、運転免許証、家族関係証明書等)を要求

- 単純な確認だけで目的の達成が可能であれば、コピーを保存してはならず、収集・保存(例：コピーを保存)が必要な場合でも収集同意を受けていない情報(例：身分証明書の裏面指紋、住民登録番号の後ろの7桁など)はマスキング処理してから収集・保存する。

例② 料金減免対象者の確認のために障害者登録証、国家有功者の証明書類などを収集する場合は、確認の目的と無関係な情報はマスキング処理して保管する。

[1] 大韓民国におけるサイバー身元確認番号体系である。一種のインターネット仮想住民登録番号

[2] 電子取引などを安心して使用できるようにするサイバー電子証明書

例③ 利用規約上の違約金免除の事由(例：引越しなど)を確認するため、事業者が必要とする人事命令書、住民登録謄本などの書類は担当者確認に代わる対策を講ずることが望ましい。

5. 段階別の個人情報破棄基準(現)

■委託者が零細業者で受託者が大規模な事業者である場合、委託者の能力を考慮して管理/監視できるように努める

■個人情報の破棄に準じて、別途分離保存/保管を追加

法では、個人情報処理者が本来の個人情報処理業務を他の事業者に委託して処理する場合、委託者に受託者の管理監督する責任を与えられるが、管理監督の代表的な行為は教育と点検にある。だが現場では受託者が委託者よりもはるかに規模が大きく、教育と点検を直接実施することは不可能に近い状況が多い。たとえばスタッフ 10人の小さなオンラインショッピングサイトが配送のために郵便局を常時利用すると、ショッピングサイトが委託者、郵便局が受託者となる。スタッフの健康診療のためにS病院を利用すると S病院が受託者となり、DM文字サービスのためにキャリアを利用すると、キャリアが受託者となる。10人規模のショッピングサイトが郵便局と S病院、キャリアの個人情報保護実態をチェックし、受託者に委託者の個人情報保護教育を受けるように要求することが可能だろうか。このような事情を考慮して、今回のガイドでは「委託者が零細事業者で、受託者が大規模な事業者で委託者の管理・監督が現実的に厳しい場合は、委託者は自身の能力を考慮して合理的な範囲内で最大限の管理・監督できるように努める」という内容が含まれた。場合によって委託者が受託者を厳密に管理監督できない状況において、規模の違いによる現実的な問題があるときは「努力」の程度によって情状酌量するという配慮が背景にある。

加えて委託に関して現場でよく聞く質問に対するガイドは以下の通りだ。

- 個人情報の委託契約書には、委託された個人情報の安全な管理と破棄及び確認事項を含めて作成する。(契約書反映内容：個人情報破棄・保護処置に関する事項のほか「定期確認事項」に関する事項等)
- 受託者が独自の事業を運用中でも、委託者から提供された個人情報について委託者の管理・監督下で、委託された範囲内のみ個人情報を処理しなければならない。(最高裁2017.4.7、判決参照)
- 個人情報の処理委託は、委託者本人の業務処理と利益のためである点を考慮すると、受託者には再受託者が含まれると見なすのが妥当であり、従って委託者も、また再受託者に対して管理・監督の責任を果たすために努め、受託者はまた再受託者への管理・監督義務を履行しなければならない。

6.理解しやすい同意書の作成基準(現)

■事業者の同意取得方法として既存の電子メール、郵便に加えて文字メッセージ、SNSなども追加

個人情報同意の確認方法として文字メッセージやソーシャルネットワークサービス(SNS)が追加されたが、文字メッセージは既に多く使われていた。Facebook、Twitterなどの SNSも利用可能である点は注目するに値する。

■ 国外の再移転時、国外移転同様の利用者同意が必要

個人情報を国外に移転する場合、情報主体の同意を受けることが法律で定められた原則だ。韓国の Bというオンラインサービスプロバイダが、米国の Aというクラウドサービスプロバイダを介して ITサービスを運営し個人情報を移転した。もちろん国外移転の会員同意を受けて行われた。ところが、米国 A社が再び他の国の C社の IDC(Internet Data Center)を利用して個人情報を移転する状況が発生した場合、これについても韓国企業 Bは、会員の同意を得なければならない。

区分	告示内容
国外移転・再移転に同意	1.移転・再移転される個人情報項目 2.個人情報が移転・再移転される国、移転日時及び移転方法 3.個人情報を移転・再移転を受ける者の氏名(法人の場合、その名称及び情報管理責任者の連絡先) 4.個人情報を移転・再移転を受ける者の個人情報利用目的と保有・利用期間

■ マーケティング活用の同意(網法第22条)と営利目的の広告性情報の受信同意(網法第50条)は別途同意

※但し、マーケティング活用の同意の横に広告性情報の受信同意有無を任意の選択同意事項に設定可能

情報通信網法第22条の同意は収集した個人情報をマーケティング目的に利用するという意思に対する合意であり、同法第50条の営利目的の広告性情報の受信同意は、具体的に広告性情報を受信することに対する同意であるため、別途の同意が必要であるという内容だ。

■個人情報の第三者への提供を受ける者が、サービス登録段階で特定されない場合は実際の購入時に告知及び同意取得が可能

第三者への提供の同意を会員登録の際に受けていない場合でも、実際の購入・決済時に告知して同意を受けることが可能であることを明示している。

購入(支払い)段階：提供を受ける第三者告示及び同意

提供を受ける者	(株) OOOO
目的	商品配送
項目	配送先の住所、連絡先
保有期間	配送完了後、X日まで
同意有無	□同意する　□同意しない

■ 必須同意項目のみで構成される場合、一括同意可能

個人情報収集の利用同意の過程で、情報主体が読むべき多くの告示事項と必須チェック同意項目は、事業者にも利用者にも面倒な存在だった。幸いなことにオンラインでは、一括同意チェックという便利な機能を実装できるため、「全体同意」というチェックボックスをよく見かける。しかし、今回の改正ガイドでは、「全体同意」による一括同意が可能な場合は、サービス利用に必要な個人情報収集の利用同意のみ可能であり、任意の選択事項まで一括処理することは原則として許可されないことを明示している。これは利用者が同意処理の利便性に誘導され、オプションの同意事項について適切な判断をしない可能性があるという点を考慮したものだろう。任意の選択事項は、多少面倒であっても個別に同意を選択できるように実装することを勧告している。

これまで改正された「オンライン個人情報ガイドライン」における重要な変更点を紹介した。4年ぶりの改正だったが、これまでの法令及び告示がかなり詳細に強化されてきたため、あえてガイドラインに盛り込む内容は多くないようだ。オンラインサービスを構築・運営する事業者の立場では、情報主体の法的権利を保護する必要が責任と、利用における利便性を確保するという課題を両立していくのが容易ではない。法律の知識がない利用者は、同意処理の多くの告知内容を読んでチェックをすることに煩わしさを感じるだろう。先の5月に発効されたGDPR(欧州一般個人情報保護法)に比べても、韓国の個人情報保護法はそのディテールと厳しさでかなり先を進んでいる。今後はさらに厳格な基準と詳細な実施基準の適用がより柔軟になることを期待する。

http://jp.ahnlab.com/site/main.do

http://global.ahnlab.com/site/main.do

http://www.ahnlab.com/kr/site/main.do

アンラボとは

株式会社アンラボは、業界をリードする情報セキュリティソリューションの開発会社です。
1995年から弊社では情報セキュリティ分野におけるイノベーターとして最先端技術と高品質のサービスをご提供できるように努力を傾けてまいりました。今後もお客様のビジネス継続性をお守りし、安心できるIT環境づくりに貢献しながらセキュリティ業界の先駆者になれるよう邁進してまいります。
アンラボはデスクトップおよびサーバー、携帯電話、オンライントランザクション、ネットワークアプライアンスなど多岐にわたる総合セキュリティ製品のラインナップを揃えております。どの製品も世界トップクラスのセキュリティレベルを誇り、グローバル向けコンサルタントサービスを含む包括的なセキュリティサービスをお届け致します。

AhnLab

〒108-0014 東京都港区芝4丁目13- 2 田町フロントビル3階 | TEL: 03-6453-8315 (代)