Meşru Menfaat Kavramının Dönüşümü: Birleşik Krallık'ın 'Tanınmış Meşru Menfaat' Modeli

I. Giriş

Kişisel verilerin korunması hukukunda "meşru menfaat" (GDPR m. 6(1)(f) ve KVKK m. 5/2(f)) her zaman en esnek, ancak aynı zamanda hukuki açıdan en tartışmalı ve yoruma açık işleme şartı olmuştur. Bu tartışmanın merkezinde ise, veri sorumlusuna yüklenen "dengeleme testi" (balancing test) — Türk hukukundaki ifadesiyle "ilgili kişinin temel hak ve özgürlüklerine zarar vermeme" koşulu — yer almaktadır.

Şimdi ise Birleşik Krallık, 2025 tarihli Veri (Kullanım ve Erişim) Yasası (DUAA) ile bu denklemi değiştiriyor. UK GDPR'a eklenen "Tanınmış Meşru Menfaat" (Recognised Legitimate Interest - RLI) adında yeni ve bağımsız bir hukuki dayanak ihdas ederek belirli senaryolar için bu dengeleme zorunluluğunu tamamen ortadan kaldırıyor.

II. "Tanınmış Meşru Menfaat" (RLI) Tam Olarak Nedir?

RLI, "meşru menfaat" (legitimate interests - 6(1)(f)) dayanağından farklı ve yeni bir hukuki dayanaktır.

Temel felsefesi şudur: Yasa koyucu, belirli işleme amaçlarının kamu yararına olduğuna ve bireyin haklarından daha ağır bastığına peşinen karar vermiştir. Eğer bir kuruluşun veri işleme amacı, yasanın Ek 1'inde listelenen bu "tanınmış" kategorilerden birine giriyorsa, kuruluşun artık geleneksel üç aşamalı meşru menfaat değerlendirmesi (LIA) ve özellikle de "dengeleme testi" yapmasına gerek kalmaz.

III. Dengeleme Testini Ortadan Kaldıran 5 "Tanınmış" Koşul

RLI, her amaca açık bir kapı değildir; yalnızca kamu yararı yüksek olan 5 spesifik koşulda geçerlidir. ICO'nun sağladığı metinlerdeki örnekler, bu koşulların pratikte nasıl işleyeceğini net bir şekilde ortaya koymaktadır.

1. Suç Koşulu (The Crime Condition): Suçun tespiti, soruşturulması, önlenmesi veya suçluların yakalanması/kovuşturulması.

Pratik Örnek: Bir sigorta şirketinin, sahte talepleri tespit etmek amacıyla analitik modeller kullanması. Normalde şirket, "dolandırıcılıkla mücadele menfaati" ile "talep sahibinin mahremiyeti" arasında bir dengeleme yapmak zorundayken, RLI sayesinde bu amaç (suç tespiti) zaten "tanınmış" kabul edilir ve dengelemeye gerek kalmaz.

2. Koruma Koşulu (The Safeguarding Condition): "Savunmasız bir bireyi" ihmalden veya fiziksel, zihinsel, duygusal zarardan korumak.

Pratik Örnek: Bir çocuk yardım kuruluşunun gençlik kulübündeki bir çocuğun davranışlarında ve görünümünde "evde fiziksel ihmale uğradığına" dair işaretler fark etmesi.

3. Acil Durum Koşulu (The Emergencies Condition): Sivil Acil Durumlar Yasası (2004) kapsamında tanımlanan ciddi, geniş çaplı acil durumlara (örn. pandemi, büyük bir sel, terör saldırısı, altyapı çöküşü) müdahale etmek.

Pratik Örnek: Bir pandemi sırasında, yerel bir topluluk grubunun, yardım hizmeti verdiği (ve konseyin listesinde olmayan) savunmasız kişilerin bilgilerini, acil destek alabilmeleri için yerel konsey (belediye) ile paylaşması.

4. Güvenlik Koşulu (National security, public security and defence condition): Ulusal güvenliği, kamu güvenliğini veya savunmayı korumak.

Pratik Örnek: Bir etkinlik şirketinin, büyük bir mekanı yönetmek (kamu güvenliği) için gerçek zamanlı CCTV izlemesi yapması.

5. Kamu Görevi İfşa Talebi Koşulu (Public task disclosure request condition): Başka bir kuruluşun (genellikle bir kamu otoritesi), kendi yasal kamu görevini yerine getirebilmesi için veri sorumlusundan veri talep etmesi durumunda, veri sorumlusunun bu veriyi paylaşması.

Pratik Örnek: Bir kamu kurumunun, bir çalışanın belirli günlerde işte olup olmadığını teyit etmek için şirkete resmi bir talepte bulunması.

IV. RLI Bir "Muafiyet" Değildir

ICO'nun net bir şekilde vurguladığı gibi, RLI bir "muafiyet" veya sınırsız bir "joker kart" değildir. Yalnızca dengeleme testini ortadan kaldıran yeni bir hukuki dayanaktır. Diğer tüm veri koruma prensipleri aynen devam etmektedir:

Gereklilik Testi Bâkidir: Veri işlemenin, bu 5 "tanınmış" amaçtan birine ulaşmak için "gerekli" (necessary) olması şarttır. Bu, işlemenin hedefli, orantılı ve amaca ulaşmak için daha az müdahaleci bir yolu yoksa yapılması gerektiği anlamına gelir.

Şeffaflık (Aydınlatma) Zorunludur: Kuruluşlar, aydınlatma metinlerinde (gizlilik bildirimi) RLI'yi yasal dayanak olarak kullandıklarını ve spesifik olarak hangi koşula (örn. "suç durumu") dayandıklarını açıkça belirtmek zorundadır.

Amaçla Sınırlılık ve Veri Minimizasyonu: Diğer tüm ilkelere (örn. veriyi amaç dışında kullanmama, gerekenden fazlasını toplamama) tam uyum şarttır.

V. İnceleme Taleplerinin Reddedilmesine Karşı Başvuru Yolları

RLI'nin en sofistike noktası, itiraz hakkı (Right to Object - Madde 21) ile olan ilişkisidir. RLI'ye dayalı işleme faaliyetlerinde veri sahibinin itiraz hakkı devam etmektedir. İtiraz mutlak değildir. Ancak, bir ilgili kişi itiraz ettiğinde, dengeleme testi "zorlayıcı meşru gerekçeler" olarak geri dönmektedir.

VI. Sonuç

Birleşik Krallık'ın bu adımı, veri koruma rejimleri arasında belirgin bir metodolojik ayrışmaya işaret etmektedir:

KVKK ve AB GDPR: "Meşru menfaat" tek bir kategoridir ve her zaman dengeleme testi gerektirir. "Peşinen kabul edilmiş" kamu yararı listesi bulunmamaktadır.

Birleşik Krallık: Meşru menfaat ikiye ayrılmıştır:
1.Standart Meşru Menfaat (Dengeleme testi gerektiren).
2.Tanınmış Meşru Menfaat (5 koşul için dengeleme testi gerektirmeyen).

Birleşik Krallık, özellikle suçla mücadele, ulusal güvenlik ve savunmasız bireylerin korunması gibi yüksek kamu yararı içeren alanlarda, veri sorumlularını (kamu ve özel sektör) dengeleme testinin hukuki belirsizliğinden kurtarmak istemektedir.

Bu, veri koruma hukukunda birey mahremiyetinden ziyade, toplumsal fayda ve hukuki kesinliğe öncelik veren daha pragmatik bir yaklaşımı temsil etmektedir. Birleşik Krallık'ın bu "önceden onaylanmış" listesi, kamu yararı ile temel haklar arasındaki dengenin nasıl farklı kurulabileceğine dair önemli bir örnek teşkil etmektedir.

The Transformation of the Legitimate Interest Concept: The United Kingdom's 'Recognised Legitimate Interest' Model

I. Introduction

In data protection law, "legitimate interest" (GDPR Art. 6(1)(f) and KVKK Art. 5/2(f)) has always been the most flexible, yet at the same time, the most legally controversial processing condition and the one most open to interpretation. At the centre of this debate lies the "balancing test" imposed on the data controller—expressed in Turkish law as the condition "not to harm the fundamental rights and freedoms of the data subject."

Now, the United Kingdom is fundamentally changing this equation with the 2025 Data (Use and Access) Act (DUAA). By introducing a new and independent legal basis added to the UK GDPR called "Recognised Legitimate Interest" (RLI), it completely eliminates this balancing requirement for certain scenarios.

II. What Exactly is "Recognised Legitimate Interest" (RLI)?

RLI is a new legal basis, distinct from the "legitimate interests" (6(1)(f)) basis.

Its core philosophy is this: The legislator has pre-determined that certain processing purposes are in the public interest and outweigh the rights of the individual. If an organisation's data processing purpose falls into one of these "recognised" categories listed in Schedule 1 of the Act, the organisation no longer needs to conduct the traditional three-stage legitimate interests assessment (LIA) and, specifically, the "balancing test."

III. The 5 "Recognised" Conditions That Eliminate the Balancing Test

RLI is not an open door for every purpose; it is valid only in 5 specific conditions with high public interest. The examples in the texts provided by the ICO clearly demonstrate how these conditions will work.

1.The Crime Condition: The detection, investigation, or prevention of crime, or the apprehension or prosecution of offenders.

Practical Example: An insurance company using analytical models to detect fraudulent claims. Normally, the company would have to balance its "interest in fraud prevention" against the "claimant's privacy," but thanks to RLI, this purpose (crime detection) is already considered "recognised," and no balancing is required.

2.The Safeguarding Condition: Protecting a "vulnerable individual" from neglect or physical, mental, or emotional harm.

Practical Example: A children's charity noticing signs in a child's behaviour and appearance at a youth club that "indicate physical neglect at home."

3.The Emergencies Condition: Responding to serious, large-scale emergencies defined under the Civil Contingencies Act (2004) (e.g., a pandemic, major flood, terrorist attack, infrastructure collapse).

Practical Example: During a pandemic, a local community group sharing information about vulnerable individuals they provide services to (who are not on the council's list) with the local council, so they can receive emergency support.

4.The National security, public security and defence condition: Protecting national security, public security, or defence.

Practical Example: An event company conducting real-time CCTV monitoring at a large venue to prevent and manage overcrowding (public security).

5. The Public task disclosure request condition: Where another organisation requests data from the data controller to fulfill its own legal public task, the data controller sharing this data.

Practical Example: A public body making an official request to a company to confirm whether an employee was at work on specific days.

IV. RLI is Not an "Exemption"

As the ICO clearly emphasizes, RLI is not an "exemption" or an unlimited "joker card." It is merely a new legal basis that removes the balancing test. All other data protection principles continue to apply:

The Necessity Test Remains: It is essential that the data processing is "necessary" to achieve one of these 5 "recognised" purposes. This means the processing must be targeted, proportionate, and undertaken only if there is no less intrusive way to achieve the purpose.

Transparency (Notification) is Mandatory: Organisations must clearly state in their privacy notices that they are using RLI as their legal basis and specify which condition (e.g., "the crime condition") they are relying on.

Purpose Limitation and Data Minimisation: Full compliance with all other principles (e.g., not using data for other purposes, not collecting more than necessary) is required.

V. The Relationship with the Right to Object

The most sophisticated point of RLI is its relationship with the Right to Object (Article 21). The data subject's right to object continues to apply to processing activities based on RLI. The objection is not absolute. However, when a data subject objects, the balancing test returns in the form of demonstrating "compelling legitimate grounds."

VI. Conclusion

The United Kingdom's move signals a clear methodological divergence among data protection regimes:

KVKK and EU GDPR: "Legitimate interest" is a single category and always requires a balancing test. There is no list of "pre-approved" public interests.

United Kingdom: Legitimate interest is divided into two:

1.Standard Legitimate Interest (Requires a balancing test).

2. Recognised Legitimate Interest (Does not require a balancing test for the 5 conditions).

The United Kingdom seeks to relieve data controllers (both public and private sector) from the legal uncertainty of the balancing test, especially in areas of high public interest such as crime prevention, national security, and the safeguarding of vulnerable individuals.

This represents a more pragmatic approach in data protection law, prioritising societal benefit and legal certainty over individual privacy. The UK's "pre-approved" list constitutes an important example of how the balance between public interest and fundamental rights can be struck differently.