İSTANBUL SABİHA GÖKÇEN ULUSLARARASI HAVALİMANI Yatırım Yapım ve İşletme A.Ş.	**İSTANBUL SABİHA GÖKÇEN ULUSLARARASI HAVALİMANI YATIRIM VE YAPIM İŞLETME A.Ş**	
	KİŞİSEL VERİ GÜVENLİĞİ POLİTİKASI	
	PERSONAL DATA SECURITY POLICY	

1. Amaç Bu Kişisel Veri Güvenliği Politikası'nın (bundan sonra "Politika" olarak anılacaktır) amacı, İstanbul Sabiha Gökçen Uluslararası Havalimanı Yatırım Yapım ve İşletme A.Ş. (bundan sonra "ISG" veya "Havalimanı" olarak anılacaktır) tarafından işlenen tüm kişisel verilerin güvenliğinin sağlanmasına yönelik çerçeveyi, 6698 sayılı Kişisel Verilerin Korunması Kanunu (KVKK), ilgili diğer mevzuat ve Kişisel Verileri Koruma Kurulu (Kurul) kararlarına uygun olarak tanımlamaktır. **2. Kapsam** Bu Politika; ● İlgili Kişi: Havalimanı yolcuları, çalışanları, çalışan adayları, ziyaretçileri, Havalimanı hizmetlerini (Wi-Fi, web sitesi, mobil uygulama, sadakat programı gibi) kullanan kişiler, kiracıların, tedarikçilerin ve diğer üçüncü tarafların personeli dahil olmak üzere kişisel verileri ISG tarafından işlenen tüm gerçek kişileri, ● Veri Kategorileri: Kimlik, iletişim, lokasyon, finansal, görsel/işitsel (CCTV kayıtları dahil), işlem güvenliği, pazarlama, sağlık (ilgili mevzuat ve koşullar dahilinde sıkı şartlara tabi olarak), biyometrik veriler ve bunlarla sınırlı olmamak üzere ISG tarafından işlenen tüm kişisel veri kategorilerini, ● İşleme Faaliyetleri: Tamamen veya	**1. Purpose** The purpose of this Personal Data Security Policy (hereinafter referred to as the "Policy") is to define the framework for ensuring the security of all personal data processed by İstanbul Sabiha Gökçen Uluslararası Havalimanı Yatırım Yapım ve İşletme A.Ş. (hereinafter referred to as "ISG" or "the Airport") , in accordance with the Law on the Protection of Personal Data No. 6698 (KVKK), other relevant legislation, and the decisions of the Personal Data Protection Board (the Board). **2. Scope** This Policy covers: • Data Subject: All natural persons whose personal data are processed by ISG, including but not limited to airport passengers, employees, employee candidates, visitors, individuals using Airport services (such as Wi-Fi, website, mobile application, loyalty program), and the personnel of tenants, suppliers, and other third parties. • Data Categories: All personal data categories processed by ISG, including but not limited to identity, contact, location, financial, visual/auditory (including CCTV recordings), transaction security, marketing, health (subject to strict conditions under relevant legislation and circumstances), and biometric data.

kısmen otomatik olan ya da herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla gerçekleştirilen tüm kişisel veri işleme faaliyetlerini,

● Coğrafi Kapsam: ISG'nin tüm yerleşkelerini ve dijital sistemlerini kapsar.

3. Tanımlar

Bu Politikada kullanılan ve aşağıda ayrıca tanımlanmayan terimler için KVKK'nın 3. maddesinde yer alan tanımlar geçerlidir. Ek olarak, Havalimanı operasyonlarına özgü terimler gerektiğinde bu Politika veya eklerinde ayrıca tanımlanabilir.

4. Veri Sorumlusu ve Temsilcisi

● Veri Sorumlusu: İstanbul Sabiha Gökçen Uluslararası Havalimanı Yatırım Yapım ve İşletme A.Ş. (Adres: Sabiha Gökçen Havalimanı Terminal Binası Pendik, İstanbul) KVKK kapsamında Veri Sorumlusu'dur.

● Veri Sorumlusu İrtibat Kişisi/Veri Koruma Görevlisi: ISG, KVKK kapsamındaki yükümlülüklerin yerine getirilmesi ve ilgili kişi başvurularının yönetilmesi amacıyla bir Veri Koruma Görevlisi atamış veya bir Kişisel Verilerin Korunması Komitesi oluşturmuştur. İrtibat bilgileri ISG'nin kurumsal web sitesinde ve Aydınlatma Metinlerinde kamuoyu ile paylaşılmaktadır.

5. Kişisel Veri İşleme İlkeleri

• Processing Activities: All personal data processing activities carried out by fully or partially automated means, or by non-automated means provided that they are part of any data recording system.

• Geographical Scope: All premises and digital systems of ISG.

3. Definitions

For terms used in this Policy that are not otherwise defined herein, the definitions provided in Article 3 of the KVKK shall apply. Additionally, terms specific to Airport operations may be separately defined in this Policy or its annexes as needed.

4. Data Controller and Representative

• Data Controller: İstanbul Sabiha Gökçen Uluslararası Havalimanı Yatırım Yapım ve İşletme A.Ş. (Address: Sabiha Gökçen Havalimanı Terminal Binası Pendik, İstanbul) is the Data Controller within the scope of the KVKK.

• Data Controller Contact Person/Data Protection Officer: ISG has appointed a Data Protection Officer or established a Personal Data Protection Committee to fulfill its obligations under the KVKK and manage data subject applications. Contact information is shared with the public on ISG's corporate website and in its Privacy Notices.

5. Principles of Personal Data Processing

İSTANBUL SABİHA GÖKÇEN ULUSLARARASI HAVALİMANI Yatırım Yapım ve İşletme A.Ş.	**İSTANBUL SABİHA GÖKÇEN ULUSLARARASI HAVALİMANI YATIRIM VE YAPIM İŞLETME A.Ş**	
	KİŞİSEL VERİ GÜVENLİĞİ POLİTİKASI	
	PERSONAL DATA SECURITY POLICY	

ISG, tüm kişisel veri işleme faaliyetlerinde KVKK'nın 4. maddesinde belirtilen aşağıdaki genel ilkelere uymayı taahhüt eder: ● Hukuka ve Dürüstlük Kurallarına Uygun Olma: Kişisel veriler, yürürlükteki mevzuata ve dürüstlük kurallarına uygun olarak işlenir. ● Doğru ve Gerektiğinde Güncel Olma: İşlenen kişisel verilerin doğruluğu ve güncelliği için azami özen gösterilir. İlgili kişilere verilerini düzeltme ve güncelleme imkânı tanınır. ● Belirli, Açık ve Meşru Amaçlar İçin İşlenme: Kişisel veriler, yalnızca önceden belirlenmiş, açık ve hukuka uygun amaçlar doğrultusunda işlenir. ● İşlendikleri Amaçla Bağlantılı, Sınırlı ve Ölçülü Olma (Veri Minimizasyonu): Kişisel veriler, belirlenen amaçların gerçekleştirilmesi için gerekli olanla sınırlı tutulur ve amaçla orantılıdır. Gereksiz veri toplanmasından kaçınılır. ● İlgili Mevzuatta Öngörülen veya İşlendikleri Amaç İçin Gerekli Olan Süre Kadar Muhafaza Edilme: Kişisel veriler, yasalarda öngörülen veya işleme amacı için gerekli olan süreler boyunca saklanır. Bu sürelerin sonunda veriler güvenli bir şekilde imha edilir. **6. Kişisel Veri İşleme Şartları (KVKK**	ISG undertakes to comply with the following general principles set forth in Article 4 of the KVKK in all its personal data processing activities: • Lawfulness and Fairness: Personal data is processed in compliance with the current legislation and the rules of fairness. • Accuracy and Being Up-to-Date Where Necessary: Utmost care is taken to ensure the accuracy and currency of the processed personal data. Data subjects are provided with the opportunity to correct and update their data. • Processing for Specific, Explicit, and Legitimate Purposes: Personal data is processed only for pre-determined, explicit, and lawful purposes. • Being Relevant, Limited, and Proportionate to the Purposes for which they are Processed (Data Minimisation): Personal data is kept limited to what is necessary for the realization of the specified purposes and is proportionate to the purpose. The collection of unnecessary data is avoided. • Retention for the Period Stipulated in the Relevant Legislation or Required for the Purpose for which they are Processed: Personal data is stored for the periods prescribed by law or required for the

Madde 5)

Kişisel veriler, KVKK'nın 5. maddesi uyarınca kural olarak ilgili kişinin açık rızası olmaksızın işlenemez. Ancak, aşağıdaki şartlardan birinin varlığı hâlinde, ilgili kişinin açık rızası aranmaksızın kişisel verilerinin işlenmesi mümkündür:

a) Kanunlarda açıkça öngörülmesi: Veri işlemenin ilgili kanunlarda açıkça zorunlu kılındığı durumlar (örneğin, Sivil Havacılık Kanunu, Kimlik Bildirme Kanunu gereği yapılan işlemeler).

b) Fiili imkânsızlık nedeniyle rızasını açıklayamayacak durumda bulunan veya rızasına hukuki geçerlilik tanınmayan kişinin kendisinin ya da bir başkasının hayatı veya beden bütünlüğünün korunması için zorunlu olması.

c) Bir sözleşmenin kurulması veya ifasıyla doğrudan doğruya ilgili olması kaydıyla, sözleşmenin taraflarına ait kişisel verilerin işlenmesinin gerekli olması: (Örneğin, yolcularla yapılan taşıma sözleşmesi kapsamında uçuş bilgilerinin işlenmesi, otel rezervasyonlarının yönetimi).

ç) Veri sorumlusunun hukuki yükümlülüğünü yerine getirebilmesi için zorunlu olması: (Örneğin, yasal mercilere yapılması gereken zorunlu bildirimler).

d) İlgili kişinin kendisi tarafından

processing purpose. At the end of these periods, the data is securely destroyed.

6. Conditions for Processing Personal Data (KVKK Article 5)

As a rule, personal data cannot be processed without the explicit consent of the data subject, pursuant to Article 5 of the KVKK. However, in the presence of one of the following conditions, it is possible to process personal data without seeking the explicit consent of the data subject:

a) It is expressly provided for by the laws (e.g., processing carried out as required by the Civil Aviation Act, the Identity Reporting Act).

b) It is necessary for the protection of life or physical integrity of the person himself/herself or of any other person who is unable to express his/her consent due to a physical disability or whose consent is not legally valid.

c) It is necessary to process personal data of the parties of a contract, provided that it is directly related to the establishment or performance of the contract (e.g., processing flight information within the scope of the carriage contract with passengers, managing hotel reservations).

ç) It is necessary for the data controller to fulfill his/her legal obligations (e.g., mandatory notifications to legal authorities).

d) The data has been made public by the data

alenileştirilmiş olması. e) Bir hakkın tesisi, kullanılması veya korunması için veri işlemenin zorunlu olması. f) İlgili kişinin temel hak ve özgürlüklerine zarar vermemek kaydıyla, veri sorumlusunun meşru menfaatleri için veri işlenmesinin zorunlu olması. Açık rızanın gerektiği durumlarda, ISG ilgili kişiyi KVKK'nın aradığı şartlara uygun olarak aydınlatacak ve özgür iradesiyle rızasını alacaktır. Alınan açık rızalar, ispatlanabilir şekilde kayıt altına alınacaktır. **7. Kişisel Verilerin Aktarılması (Yurt İçi ve Yurt Dışı)** ISG tarafından işlenen kişisel veriler, KVKK'nın 8. (yurt içi aktarım) ve 9. (yurt dışı aktarım) maddelerinde belirtilen şartlara uygun olarak üçüncü kişilere aktarılabilecektir. ● Yurt İçi Aktarım: Kişisel veriler, KVKK Madde 5(2)'de belirtilen işleme şartlarından birinin varlığı halinde veya bu şartlar yoksa ilgili kişinin açık rızası alınmak suretiyle yurt içindeki üçüncü kişilere (örneğin, yetkili kamu kurum ve kuruluşları, iş ortakları, tedarikçiler) aktarılabilir. ● Yurt Dışı Aktarım: Kişisel verilerin yurt dışına aktarımı, aşağıdaki koşullardan birinin sağlanmasıyla mümkündür:	subject himself/herself. e) Data processing is necessary for the establishment, exercise, or protection of any right. f) It is necessary for the legitimate interests of the data controller, provided that the fundamental rights and freedoms of the data subject are not harmed. In cases where explicit consent is required, ISG will inform the data subject in accordance with the conditions stipulated by the KVKK and obtain their consent based on their free will. The explicit consents obtained will be recorded in a provable manner. **7. Transfer of Personal Data (Domestic and International)** Personal data processed by ISG may be transferred to third parties in accordance with the conditions specified in Articles 8 (domestic transfer) and 9 (international transfer) of the KVKK. Domestic Transfer: Personal data may be transferred to third parties within the country (e.g., authorized public institutions and organizations, business partners, suppliers) if one of the processing conditions specified in KVKK Article 5(2) exists, or if these conditions are not met, by obtaining the explicit consent of the data subject. International Transfer: The transfer of personal

○ İlgili kişinin açık rızasının bulunması. ○ Aktarım yapılacak ülkede yeterli korumanın bulunması (Kurul tarafından ilan edilen ülkeler). ○ Aktarım yapılacak ülkede yeterli koruma bulunmuyorsa, ISG ve ilgili ülkedeki veri sorumlusunun/veri işleyenin yeterli bir korumayı yazılı olarak taahhüt etmesi ve Kurul'un izninin bulunması. ○ KVKK Madde 5(2) ve Madde 6(3)'te belirtilen şartların varlığı ve yeterli korumanın bulunduğu ülkelere veya yeterli korumayı taahhüt eden ve Kurul izni olan veri sorumlularına aktarım. (Örneğin, çalışan adayı verilerinin yurt dışındaki topluluk şirketlerine veya tedarikçilere aktarımı için standart sözleşme gibi güvenceler). Havalimanı operasyonlarının uluslararası niteliği (uluslararası uçuşlar, yabancı havayolları ile işbirliği, global hizmet sağlayıcılar) göz önüne alındığında, yurt dışı veri transferi süreçleri özel bir dikkat ve titizlikle yönetilecektir. **8. Kişisel Veri Güvenliğine İlişkin Yükümlülükler (KVKK Madde 12)** ISG, KVKK'nın 12. maddesi uyarınca; ● Kişisel verilerin hukuka aykırı olarak işlenmesini önlemek, ● Kişisel verilere hukuka aykırı olarak	data abroad is possible if one of the following conditions is met: The explicit consent of the data subject is obtained. There is adequate protection in the country to which the data will be transferred (countries announced by the Board). If there is no adequate protection in the destination country, ISG and the data controller/data processor in the relevant country provide a written commitment for adequate protection, and the permission of the Board is obtained. The conditions specified in KVKK Article 5(2) and Article 6(3) are met, and the transfer is made to countries with adequate protection or to data controllers who have committed to adequate protection and obtained the Board's permission. (e.g., safeguards such as standard contractual clauses for the transfer of employee candidate data to group companies or suppliers abroad). Given the international nature of airport operations (international flights, cooperation with foreign airlines, global service providers), international data transfer processes will be managed with special care and diligence. **8. Obligations Regarding Personal Data Security (KVKK Article 12)** Pursuant to Article 12 of the KVKK, ISG is

erişilmesini önlemek,

- Kişisel verilerin muhafazasını sağlamak

amacıyla uygun güvenlik düzeyini temin etmeye yönelik gerekli her türlü teknik ve idari tedbirleri almakla yükümlüdür. Bu tedbirler, Kurul tarafından yayımlanan "Kişisel Veri Güvenliği Rehberi (Teknik ve İdari Tedbirler)" esas alınarak belirlenmiş ve aşağıda detaylandırılmıştır.

8.1. İdari Tedbirler

ISG, kişisel verilerin güvenliğini sağlamak amacıyla aşağıdaki idari tedbirleri alır ve uygular:

- Kişisel Veri İşleme Envanteri Hazırlanması: Havalimanı bünyesinde gerçekleştirilen tüm kişisel veri işleme faaliyetlerinin, amaçlarının, hukuki sebeplerinin, veri kategorilerinin, aktarılan alıcı gruplarının ve saklama sürelerinin detaylı bir şekilde belirlendiği bir Kişisel Veri İşleme Envanteri hazırlanır ve güncel tutulur.

- Kurumsal Politikaların Oluşturulması ve Uygulanması: Bu Politika başta olmak üzere, erişim, bilgi güvenliği, kullanım, saklama ve imha gibi konularda detaylı kurumsal politikalar (örneğin, Veri Saklama ve İmha Politikası) oluşturulur, çalışanlara duyurulur ve uygulanması sağlanır.

- Sözleşme Yönetimi: Veri işleyenler ve

obligated to take all necessary technical and administrative measures to ensure the appropriate level of security in order to:

- Prevent the unlawful processing of personal data,
- Prevent unlawful access to personal data,
- Ensure the preservation of personal data.

These measures have been determined based on the "Personal Data Security Guide (Technical and Administrative Measures)" published by the Board and are detailed below.

8.1. Administrative Measures

ISG takes and implements the following administrative measures to ensure the security of personal data:

- Preparation of a Personal Data Processing Inventory: A Personal Data Processing Inventory is prepared and kept up-to-date, detailing all personal data processing activities carried out within the Airport, their purposes, legal grounds, data categories, recipient groups to whom data is transferred, and storage periods.
- Creation and Implementation of Corporate Policies: Detailed corporate policies concerning access, information security, use, storage, and destruction (e.g., Data Retention and

kişisel veri aktarımı yapılan üçüncü taraflarla KVKK uyumlu, veri güvenliği yükümlülüklerini içeren sözleşmeler akdedilir.

- Gizlilik Taahhütnameleri: Kişisel verilere erişimi olan çalışanlardan ve üçüncü taraf personelden gizlilik taahhütnameleri alınır.

- Kurum İçi Periyodik ve/veya Rastgele Denetimler: KVKK uyumunun ve uygulanan tedbirlerin etkinliğinin değerlendirilmesi amacıyla düzenli iç denetimler yapılır veya yaptırılır.

- Risk Analizleri ve Tehdit Değerlendirmeleri: Kişisel veri güvenliğine ilişkin riskler ve tehditler periyodik olarak değerlendirilir ve bu riskleri azaltmaya yönelik önlemler planlanır.

- Eğitim ve Farkındalık Faaliyetleri: Tüm çalışanlara ve ilgili üçüncü taraf personeline, KVKK, bilgi güvenliği ve kişisel verilerin korunması konularında düzenli eğitimler verilir ve farkındalık artırıcı faaliyetler düzenlenir.

- Veri Sorumluları Sicil Bilgi Sistemine (VERBİS) Bildirim: Yasal yükümlülükler çerçevesinde VERBİS'e kayıt ve bildirim işlemleri zamanında yerine getirilir.

- Yetki Matrisi Oluşturulması ve Uygulanması: Çalışanların kişisel verilere erişim yetkileri, görev tanımları ve "bilmesi gereken" prensibi doğrultusunda bir Yetki

Disposal Policy) are created, particularly this Policy, announced to employees, and their implementation is ensured.

- Contract Management: Contracts that comply with the KVKK and include data security obligations are concluded with data processors and third parties to whom personal data is transferred.
- Confidentiality Undertakings: Confidentiality undertakings are obtained from employees and third-party personnel who have access to personal data.
- Periodic and/or Random Internal Audits: Regular internal audits are conducted or commissioned to assess KVKK compliance and the effectiveness of the implemented measures.
- Risk Analyses and Threat Assessments: Risks and threats to personal data security are periodically assessed, and measures to mitigate these risks are planned.
- Training and Awareness Activities: Regular training on the KVKK, information security, and the protection of personal data is provided to all employees and relevant third-party personnel, and awareness-raising activities are organized.
- Notification to the Data Controllers' Registry Information System (VERBİS): Registration and

Matrisi ile belirlenir ve uygulanır. Erişim yetkileri düzenli olarak gözden geçirilir.

● Görev Değişikliği veya İşten Ayrılma Durumlarında Yetki Kaldırma: Görevinden ayrılan veya görevi değişen personelin kişisel verilere erişim yetkileri derhal kaldırılır ve zimmetindeki veri içeren envanterler iade alınır.

● Kişisel Veri Güvenliği İhlallerinin Raporlanması ve Yönetimi Prosedürleri: Olası bir kişisel veri ihlali durumunda izlenecek adımları, sorumlulukları ve bildirim süreçlerini içeren bir Veri İhlali Müdahale Planı oluşturulur ve uygulanır.

● Veri Koruma Görevlisi/Komitesi Atanması: KVKK uyum süreçlerini koordine etmek, politikaların uygulanmasını takip etmek ve ilgili kişi başvurularını yönetmek üzere bir Veri Koruma Görevlisi atanır veya bir Kişisel Verilerin Korunması Komitesi kurulur.

8.2. Teknik Tedbirler

ISG, kişisel verilerin teknik güvenliğini sağlamak amacıyla aşağıdaki teknik tedbirleri alır ve uygular:

● Siber Güvenliğin Sağlanması: Ağ güvenliği (güvenlik duvarları, ağ segmentasyonu vb.) ve uygulama güvenliği (güvenli yazılım geliştirme prensipleri, düzenli zafiyet taramaları vb.) sağlanır.

notification procedures to VERBİS are carried out in a timely manner within the framework of legal obligations.

- Creation and Implementation of an Authorization Matrix: Employees' access rights to personal data are determined and implemented through an Authorization Matrix in line with their job descriptions and the "need-to-know" principle. Access rights are reviewed regularly.
- Revocation of Authority in Case of Change of Position or Termination of Employment: The access rights of personnel who leave their position or whose position changes are immediately revoked, and any inventory containing data in their possession is returned.
- Procedures for Reporting and Managing Personal Data Security Breaches: A Data Breach Incident Response Plan is created and implemented, which includes the steps to be followed, responsibilities, and notification processes in the event of a possible personal data breach.
- Appointment of a Data Protection Officer/Committee: A Data Protection Officer is appointed or a Personal Data Protection Committee is established to coordinate KVKK compliance processes, monitor the implementation of policies, and manage data subject

- Kişisel Veri Güvenliğinin Takibi: Bilgi sistemlerine yönelik risk, tehdit, zafiyet ve açıklıkları ortaya çıkarmak ve gerekli önlemleri almak amacıyla düzenli olarak sızma (penetrasyon) testleri yapılır veya yaptırılır. Sistemlerdeki anormal aktiviteler ve olası sızma girişimleri izlenir. Erişim logları ve işlem hareketleri kayıtları (log kayıtları) düzenli ve güvenli bir şekilde tutulur.

- Erişim Yetki ve Kontrol Sistemleri: Kişisel verilere erişim, yetki matrisine uygun olarak "bilmesi gereken" ve "en az yetki" prensiplerine göre sınırlandırılır. Kullanıcı kimlik doğrulama mekanizmaları (güçlü parolalar, çok faktörlü kimlik doğrulama) kullanılır.

- Veri Kaybı Önleme (DLP) Yazılımları: Hassas kişisel verilerin kurum dışına yetkisiz çıkışını engellemek veya tespit etmek amacıyla Veri Kaybı Önleme (DLP) çözümleri kullanılır veya planlanır.

- Şifreleme (Kriptografi): Özellikle hassas kişisel veriler ve özel nitelikli kişisel veriler başta olmak üzere, risk değerlendirmesi sonucunda gerekli görülen kişisel veriler, hem depolanırken (at-rest) hem de aktarılırken (in-transit) uygun kriptografik yöntemlerle şifrelenir.

- Güncel Anti-Virüs Sistemleri ve Güvenlik Duvarları: Tüm sunucu, istemci bilgisayarlar ve ağ sistemlerinde güncel anti-virüs yazılımları ve yapılandırılmış güvenlik applications.

The EK-1 table summarizes the main administrative measures to be implemented by ISG and their responsibilities.

8.2. Technical Measures

ISG takes and implements the following technical measures to ensure the technical security of personal data:

- **Ensuring Cyber Security:** Network security (firewalls, network segmentation, etc.) and application security (secure software development principles, regular vulnerability scans, etc.) are provided.
- **Monitoring of Personal Data Security:** Penetration tests are regularly conducted or commissioned to identify risks, threats, vulnerabilities, and exposures related to information systems and to take necessary precautions. Abnormal activities and potential intrusion attempts on systems are monitored. Access logs and transaction records (log records) are kept regularly and securely.
- **Access Authorization and Control Systems:** Access to personal data is restricted according to the authorization matrix based on the "need-to-know" and "least privilege" principles. User authentication

duvarları kullanılır.

● Veri Yedekleme Stratejileri: Kişisel verilerin kaybolması veya zarar görmesi riskine karşı düzenli yedekleme yapılır. Yedeklenen kişisel veriler, ana sistemlerden ayrı ve güvenli ortamlarda (tercihen ağ dışında) saklanır ve yalnızca yetkili sistem yöneticileri tarafından erişilebilir.

● Fiziksel Güvenlik Önlemleri: Kişisel verilerin saklandığı sunucu odaları, arşivler gibi fiziksel ortamların yangın, sel, hırsızlık, yetkisiz giriş gibi risklere karşı güvenliği sağlanır.

● Kullanıcı Hesap Yönetimi: Kullanıcı hesapları (oluşturma, yetkilendirme, kapatma) merkezi olarak yönetilir ve düzenli olarak denetlenir.

● Saldırı Tespit ve Önleme Sistemleri (IDS/IPS): Ağ trafiğini ve sistem aktivitelerini izleyerek olası saldırıları tespit eden ve engelleyen sistemler kullanılır.

● Güvenli Protokoller (HTTPS): ISG'ye ait web siteleri ve online platformlarda veri iletişiminin güvenliği için HTTPS gibi güvenli protokoller kullanılır.

● Mobil Cihaz Güvenliği: Çalışanlara tahsis edilen veya kişisel verilerin işlendiği mobil cihazlar için güvenlik politikaları (şifreleme, uzaktan silme vb.) uygulanır.

● Kağıt Ortamındaki Verilerin

mechanisms (strong passwords, multi-factor authentication) are used.

- **Data Loss Prevention (DLP) Software:** Data Loss Prevention (DLP) solutions are used or planned to prevent or detect the unauthorized exfiltration of sensitive personal data from the organization.
- **Encryption (Cryptography):** Personal data deemed necessary as a result of risk assessment, especially sensitive personal data and special categories of personal data, are encrypted with appropriate cryptographic methods both at-rest and in-transit.
- **Up-to-Date Anti-Virus Systems and Firewalls:** Up-to-date anti-virus software and configured firewalls are used on all servers, client computers, and network systems.
- **Data Backup Strategies:** Regular backups are performed against the risk of loss or damage to personal data. Backed-up personal data is stored in separate and secure environments (preferably offline) and is accessible only by authorized system administrators.
- **Physical Security Measures:** The security of physical environments where personal data is stored, such as server rooms and archives, is ensured against risks like fire, flood, theft, and unauthorized access.

Güvenliği: Kağıt ortamında bulunan kişisel verilerin yetkisiz erişime, kaybolmaya veya çalınmaya karşı korunması için gerekli fiziksel güvenlik önlemleri (kilitli dolaplar, kontrollü erişim vb.) alınır.

EK-2'deki tablo, ISG tarafından uygulanacak temel teknik tedbirleri ve uygulama alanlarını özetlemektedir.

9. İlgili Kişinin Hakları (KVKK Madde 11)

Kişisel verisi işlenen her gerçek kişi (İlgili Kişi), KVKK'nın 11. maddesi uyarınca aşağıdaki haklara sahiptir:

- Kişisel veri işlenip işlenmediğini öğrenme,
- Kişisel verileri işlenmişse buna ilişkin bilgi talep etme,
- Kişisel verilerin işlenme amacını ve bunların amacına uygun kullanılıp kullanılmadığını öğrenme,
- Yurt içinde veya yurt dışında kişisel verilerin aktarıldığı üçüncü kişileri bilme,
- Kişisel verilerin eksik veya yanlış işlenmiş olması hâlinde bunların düzeltilmesini isteme ve bu kapsamda yapılan işlemin kişisel verilerin aktarıldığı üçüncü kişilere bildirilmesini isteme,
- KVKK ve ilgili diğer kanun hükümlerine uygun olarak işlenmiş olmasına rağmen, işlenmesini gerektiren sebeplerin

- **User Account Management:** User accounts (creation, authorization, closure) are managed centrally and audited regularly.
- **Intrusion Detection and Prevention Systems (IDS/IPS):** Systems that monitor network traffic and system activities to detect and prevent potential attacks are used.
- **Secure Protocols (HTTPS):** Secure protocols such as HTTPS are used for the security of data communication on ISG's websites and online platforms.
- **Mobile Device Security:** Security policies (encryption, remote wipe, etc.) are applied to mobile devices assigned to employees or used for processing personal data.
- **Security of Data in Paper Form:** Necessary physical security measures (locked cabinets, controlled access, etc.) are taken to protect personal data in paper form against unauthorized access, loss, or theft.

The EK-2 table summarizes the main technical measures to be implemented by ISG and their areas of application.

9. Rights of the Data Subject (KVKK Article 11)

Every natural person whose personal data is processed (Data Subject) has the following rights under Article 11 of the KVKK:

ortadan kalkması hâlinde kişisel verilerin silinmesini veya yok edilmesini isteme ve bu kapsamda yapılan işlemin kişisel verilerin aktarıldığı üçüncü kişilere bildirilmesini isteme,

- İşlenen verilerin münhasıran otomatik sistemler vasıtasıyla analiz edilmesi suretiyle kişinin kendisi aleyhine bir sonucun ortaya çıkmasına itiraz etme,

- Kişisel verilerin kanuna aykırı olarak işlenmesi sebebiyle zarara uğraması hâlinde zararın giderilmesini talep etme.

10. Başvuru Usulü

İlgili kişiler, KVKK Madde 11 kapsamındaki haklarına ilişkin taleplerini, "Veri Sorumlusuna Başvuru Usul ve Esasları Hakkında Tebliğ"e uygun olarak aşağıdaki yöntemlerle ISG'ye iletebilirler:

- Yazılı Başvuru: Islak imzalı dilekçe ile şahsen veya noter kanalıyla "Sabiha Gökçen Havalimanı Terminal Binası Pendik, İstanbul" adresine.

- Kayıtlı Elektronik Posta (KEP) ile Başvuru: ISG'nin KEP adresine.

- E-posta Yoluyla Başvuru: Daha önce ISG'ye bildirilen ve sistemde kayıtlı bulunan elektronik posta adresini kullanarak [kvkk@sgia.aero] adresine veya güvenli elektronik imza/mobil imza ile imzalanmış bir

- To learn whether their personal data is processed or not,

- To request information if their personal data has been processed,

- To learn the purpose of the processing of their personal data and whether they are used in conformity with the purpose,

- To know the third parties to whom their personal data is transferred in the country or abroad,

- To request the rectification of the incomplete or inaccurate data, if any, and to request reporting of the rectification to the third parties to whom the personal data has been transferred,

- To request the erasure or destruction of personal data in the event that the reasons for its processing cease to exist, despite being processed in accordance with the KVKK and other relevant laws, and to request reporting of the operation carried out in this context to the third parties to whom the personal data has been transferred,

- To object to the emergence of a result against the person himself/herself by analyzing the data processed solely through automated systems,

e-posta ile.

● Başvuru Formu: ISG'nin kurumsal web sitesinde yayınlanacak olan "İlgili Kişi Başvuru Formu" doldurularak yukarıdaki yöntemlerden biriyle iletilebilir.

Başvurularda, talebin açık ve anlaşılır olması, kimliği tevsik edici belgelerin (T.C. kimlik numarası, yabancılar için uyruk ve pasaport/kimlik numarası vb.) eklenmesi ve talebin başvuru sahibiyle ilgili olması gerekmektedir. Başkası adına yapılan başvurularda özel yetkili vekaletname sunulmalıdır.

ISG, usulüne uygun yapılan başvuruları, talebin niteliğine göre en kısa sürede ve en geç otuz gün içinde ücretsiz olarak sonuçlandıracaktır. Ancak, işlemin ayrıca bir maliyet gerektirmesi hâlinde, Kurulca belirlenen tarifedeki ücret talep edilebilir.

11. Veri İhlali Yönetimi

ISG, işlenen kişisel verilerin kanuni olmayan yollarla başkaları tarafından elde edilmesi (veri ihlali) durumunda, bu durumu öğrendiği tarihten itibaren gecikmeksizin ve en geç 72 saat içinde Kişisel Verileri Koruma Kurulu'na ve ilgili İlgili Kişine bildirmekle yükümlüdür. Bu amaçla, veri ihlallerinin tespiti, değerlendirilmesi, raporlanması ve giderilmesine yönelik bir "Veri İhlali Müdahale Planı" oluşturulmuş ve yürürlüktedir. Bu plan, sorumlulukları, iletişim kanallarını ve atılacak adımları detaylı bir

- To claim compensation for the damage arising from the unlawful processing of personal data.

10. Application Procedure

Data subjects may submit their requests regarding their rights under KVKK Article 11 to ISG using the following methods, in accordance with the "Communiqué on the Procedures and Principles of Application to the Data Controller":

- **Written Application:** In-person with a wet-signed petition or via a notary to the address "Sabiha Gökçen Havalimanı Terminal Binası Pendik, İstanbul".
- **Application via Registered Electronic Mail (KEP):** To ISG's KEP address.
- **Application via E-mail:** By using the e-mail address previously notified to ISG and registered in its system to [kvkk@sgia.aero], or via an e-mail signed with a secure electronic signature/mobile signature.
- **Application Form:** By filling out the "Data Subject Application Form" to be published on ISG's corporate website and submitting it via one of the methods above.

In applications, the request must be clear and

şekilde tanımlar.

12. Politikanın Gözden Geçirilmesi ve Güncellenmesi

Bu Politika, ISG Yönetimi tarafından onaylandığı tarihte yürürlüğe girer. Politika, KVKK ve ilgili mevzuattaki değişiklikler, Kurul kararları, yargı içtihatları ve ISG'nin veri işleme faaliyetlerindeki önemli değişiklikler doğrultusunda düzenli olarak (en az yılda bir kez) gözden geçirilir ve gerekli güncellemeler yapılır. Güncellenen Politika, ISG'nin kurumsal web sitesinde yayınlanır ve çalışanlara duyurulur.

13. Yürürlük

Bu Politika, ISG Yönetimi'nin onayı ile yürürlüğe girmiştir.

understandable, documents verifying identity (T.C. ID number, nationality and passport/ID number for foreigners, etc.) must be attached, and the request must pertain to the applicant. For applications made on behalf of another person, a special power of attorney must be submitted.

ISG will conclude duly submitted applications free of charge as soon as possible and within thirty days at the latest, depending on the nature of the request. However, if the transaction requires an additional cost, the fee in the tariff determined by the Board may be charged.

11. Data Breach Management

In the event that processed personal data is obtained by others through unlawful means (data breach), ISG is obligated to notify the Personal Data Protection Board and the relevant Data Subject without delay and within 72 hours at the latest from the date it becomes aware of the situation. For this purpose, a "Data Breach Incident Response Plan" has been established and is in effect for the detection, assessment, reporting, and remediation of data breaches. This plan defines responsibilities, communication channels, and the steps to be taken in detail.

12. Policy Review and Update

This Policy enters into force on the date it is approved by the ISG Management. The Policy is reviewed regularly (at least once a year) and

	updated as necessary in line with changes in the KVKK and related legislation, Board decisions, judicial precedents, and significant changes in ISG's data processing activities. The updated Policy is published on ISG's corporate website and announced to employees. **13. Entry into Force** This Policy was approved by the ISG's Management and entered into force.

EK-1: Uygulanacak İdari Tedbirler

Tedbir No.	Tedbir Açıklaması	Sorumlu Departman/Birim	Uygulama Takvimi/Durumu	Referans (KVKK Rehberi, Politika Md.)
İT-01	Kişisel Veri İşleme Envanteri Hazırlanması ve Güncellenmesi	Hukuk Müşavirliği, Bilgi Teknolojileri, İlgili İş Birimleri	Sürekli	KVKK Rehberi, Politika Md. 8.1
İT-02	Kurumsal Politikaların (Saklama-İmha vb.)	Hukuk Müşavirliği, Uyum Departmanı	Tamamlandı	KVKK Rehberi, Politika Md. 8.1

	Oluşturulması			
İT-03	Veri İşleyenlerle KVKK Uyumlu Sözleşmeler Yapılması	Hukuk Müşavirliği, Satın Alma Departmanı	Sürekli	KVKK Rehberi, Politika Md. 8.1
İT-04	Çalışanlara KVKK ve Bilgi Güvenliği Eğitimleri Verilmesi	İnsan Kaynakları, Bilgi Teknolojileri	Yıllık/İhtiyaç Halinde	KVKK Rehberi, Politika Md. 8.1
İT-05	Yetki Matrisi Oluşturulması ve Gözden Geçirilmesi	Bilgi Teknolojileri, İlgili İş Birimleri	Yıllık/Sürekli	Politika Md. 8.1
İT-06	Veri İhlali Müdahale Planı Oluşturulması ve Test Edilmesi	Bilgi Teknolojileri, Hukuk Müşavirliği	Tamamlandı/Yıllık Test	KVKK Rehberi, Politika Md. 11
İT-07	VERBİS Kayıt ve Bildirim Yükümlülüklerinin Takibi	Hukuk Müşavirliği, Uyum Departmanı	Yasal Sürelere Uygun	KVKK Rehberi
İT-08	Kurum İçi Periyodik Denetimler Yapılması	İç Denetim/Uyum Departmanı	Yıllık	Politika Md. 8.1

EK-2: Uygulanacak Teknik Tedbirler

Tedbir No.	Tedbir Açıklaması	Uygulandığı Sistem/Alan	Sorumlu Departman/ Birim	Periyodik Kontrol Sıklığı	Referans (KVKK Rehberi, Politika Md.)
TT-01	Güvenlik Duvarları ve Ağ Segmentasyonu	Havalimanı Ağı, Sunucu Sistemleri	Bilgi Teknolojileri	Sürekli/Yıllık Gözden Geçirme	KVKK Rehberi, Politika Md. 8.2
TT-02	Sızma (Penetrasyon) Testleri	Dışa Açık Sistemler, Kritik Veri Tabanları	Bilgi Teknolojileri	Yıllık/İhtiyaç Halinde	KVKK Rehberi, Politika Md. 8.2
TT-03	Erişim Yetki ve Kontrolü (Çok Faktörlü Kimlik Doğrulama)	Tüm Bilgi Sistemleri, Veri Tabanları	Bilgi Teknolojileri	Sürekli	KVKK Rehberi, Politika Md. 8.2
TT-04	Veri Şifreleme (Depolama ve Aktarımda)	Hassas Veri Tabanları, Özel Nitelikli Veriler, Yedekler	Bilgi Teknolojileri	Uygulama Bazlı	KVKK Rehberi, Politika Md. 8.2
TT-05	Güncel	Tüm	Bilgi	Sürekli	Politika Md.

	Anti-Virüs ve Kötü Amaçlı Yazılım Koruması	Sunucular ve İstemci Bilgisayarlar	Teknolojileri		8.2
TT-06	Veri Yedekleme ve Kurtarma	Tüm Kritik Sistemler ve Veri Tabanları	Bilgi Teknolojileri	Günlük/Haftalık	KVKK Rehberi, Politika Md. 8.2
TT-07	Log Yönetimi ve Analizi	Ağ Cihazları, Sunucular, Kritik Uygulamalar	Bilgi Teknolojileri	Sürekli	KVKK Rehberi, Politika Md. 8.2
TT-08	Fiziksel Ortam Güvenliği (Sunucu Odaları vb.)	Veri Merkezleri, Sunucu Odaları, Arşivler	Bilgi Teknolojileri, İdari İşler	Sürekli	KVKK Rehberi, Politika Md. 8.2

İSTANBUL SABİHA GÖKÇEN ULUSLARARASI HAVALİMANI Yatırım Yapım ve İşletme A.Ş.	**İSTANBUL SABİHA GÖKÇEN ULUSLARARASI HAVALİMANI YATIRIM VE YAPIM İŞLETME A.Ş**	
	KİŞİSEL VERİ GÜVENLİĞİ POLİTİKASI	
	PERSONAL DATA SECURITY POLICY	