

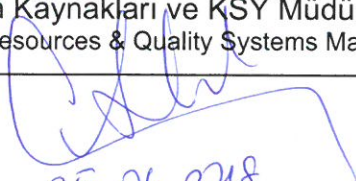
**KİŞİSEL VERİLERİN
KORUNMASI VE İŞLENMESİ
POLİTİKASI**

**Personal Data Protection
And
Processing Policy**

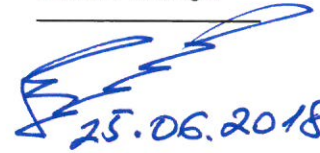
Bilgi İşlem Müdürü
IT Manager


S. GENİŞ
22. Haziran 2018

İnsan Kaynakları ve KSY Müdürü
Human Resources & Quality Systems Manager


25.06.2018
Can Alemdar

Genel Müdür
General Manager


25.06.2018

Kod No : BIY.BIP00002
Rev. No: 0
İlk Yayın Tarihi: 19.6.2018
Revizyon Tarihi : 19.6.2018

GİRİŞ **PREAMBLE**

Bu çalışma 6698 Sayılı Kişisel Verilerin Korunması Kanunu ve ilgili mevzuat gereğince şirketlerin yapması gereken değişiklikler, süreçler, takip edilecek yolları göstermek amacıyla yapılmış olan bir çalışmadır.

This work sets forth the amendments, processes, methods to be followed by the companies as per Personal Data Protection Law no. 6698 and the relevant legislation.

İşbu Politika, şirketler tarafından kişisel verilerin korunması ve hukuka uygun işlenmesi için benimsenecek ve içselleştirilecek idari yapı, süreç ve prosedürleri ifade etmektedir.

This Policy refers to an administrative structure, process and procedures to be adopted and internalized for protecting and processing the personal data in compliance with the law by the companies.

İşbu Politika'nın amacı, kişisel verilerin güvenliği ve korunması hususunda gerekli teknik ve idari önlemlerin alınarak, kişisel verilerin 6698 Sayılı Kişisel Verilerin Korunması Kanunu'na ("KVKK" veya "Kanun") uyumlu olarak işlenmesinin ve tutulmasının içselleştirilmesi ve çalışanlar ve tüm iş ortaklarında gerekli farkındalığın yaratılarak Kanun'a uyum sağlanmasıdır.

Purpose of this Law is to ensure internalization of processing and retention of the personal data in compliance with Personal Data Protection Law no. 6698 ("KVKK" or "Law") by adopting required technical and administrative measures in the field of safety and protection of personal data and to adapt to the Law by raising required awareness in all business partners.

Şirketlerin iş ve işlemleri süresince kişisel verilerin yasal gerekliliklere uygun olarak ele alınması ve uygunluğun sağlanması amacıyla hem kendi içinde hem de mümkün olduğu sürece Şirketlerin verileri dâhil bunlar tarafından sağlanan verileri işleyen üçüncü kişiler tarafından makul adımların atılmasını sağlama sorumluluğu bulunmaktadır.

The Companies are responsible for ensuring taking reasonable steps by third parties processing the data provided by the companies including their data within their bodies and as far as possible for procuring handling of the personal data in compliance with the legal requirements and their compliance throughout the works and procedures.

Şirketler bu sorumluluğunun bilinci içerisinde verilerin Kanun'un gerektirdiği ölçüde güvenle korunması için gereken adımları uygulamalıdır.

The Companies should implement the required steps for protecting the data in confidence to be extent required by the law by being aware of this responsibility.

TANIMLAR **DEFINITIONS**

Şirket: Şirket topluluğu, iştirakler, işbirliği içindeki şirket v.b. ifade etmektedir.

Company: *refers to the Company Group, affiliates and the company within the collaboration.*

Veri: Elektronik olarak bilgisayarda ya da bir takım kâğıt bazlı dosyalama sistemlerinde saklanan bilgileri ifade etmektedir.

Data: *refers to the information stored electronically in a computer or a series of paper-based filing system.*

Kişisel Veri: Kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgiyi ifade etmektedir. Şirketler, müşteri tercihlerini anlamak ve daha iyi hizmet vermek ve benzeri amaçlar ile internet siteleri aracılığıyla, genel olarak "web kayıt bilgisi" adı verilen verileri (kullanıcıların internet tarayıcılarına, mobil cihazlarına, işletim sistemine, ziyaret ettiği sayfalara, bu sayfalara eriştiği diğer internet sayfalarına, ilgili internet sitesini ziyaret ettiği tarih ve zamana, ziyaret edilen spesifik sayfalara ve daha fazlasına ait bilgiler ve benzerlerini) toplayabilir ve internet sitesinde yer alan sayfaların ziyaret edilmesi halinde, çerezleri (cookies) kullanabilir. Bu kapsamda Kişisel Veri elde edilmesi ya da bu yol ile toplanan verilerin birlikte işlenmesi halinde belirli bir kişiye işaret etmeleri durumunda, çerezler ve web kayıt bilgileri de işbu Politika'ya tabi olacaktır.

Personal Data: *refers to any information related to the identified or identifiable real person. The Companies may collect the data called "web internet sites" through Internet web sites for the purpose of understanding the customer preferences and providing better service and similar purposes thereof (the information and like pertaining to Internet browsers of users, mobile devices, operating system, visited pages, other Internet pages accessed to these pages, date and time visiting the relevant*

Internet web site, visited specific pages and more information and may use the cookies for visiting the pages on the web site. In this context, the cookies and web registry information shall subject to this Policy if Personal data is obtained or the data collected by this means is processed together when they signal a specific person.

Özel Nitelikli / Hassas Kişisel Veri: Irka, etnik kökene, siyasi düşüncelere, felsefi inanca, dine, mezhebe veya diğer inançlara, kılık ve kıyafete, dernek, vakıf ya da sendika üyeliklerine, sağlığa, cinsel hayata, ceza mahkûmiyeti ve güvenlik tedbirlerine ve biyometrik verilere ilişkin verileri ifade etmektedir. Hassas veriler sadece sıkı şartlar altında işlenebilirler ve işlenmesi genellikle veri sahibinin açık rızasını gerektirmektedir.

Special Quality / Sensitive personal data: *refers to the data relating to race, ethnic origin, political opinion, philosophical belief, religion, sect or other beliefs, costumes and outfit, associations or foundations or trade union membership, health, sexual life, criminal conviction and safety measures and biometric data. Sensitive data can only be processed under strict conditions and their processing often requires the express consent of the data owner.*

Veri İlgilisi veya Sahipleri: Kişisel Verileri şirket tarafından işlenen çalışanlar dahil tüm gerçek kişileri kapsamaktadır. Veri sahibi Türk vatandaşı olmak ya da Türkiye’de ikamet etmek zorunda değildir. Tüm veri sahipleri, kendi kişisel verilerine ilişkin yasal haklara sahiptir.

Data Relevant Person or Owners: *Personal data covers all real persons including the employees processed by the Company. Data owner does not have to be a Turkish citizen or does not have to reside in Turkey. All data owners are entitled legal rights relating to their personal data.*

Veri Sorumlusu: Kişisel verilerin işleme amaçlarını ve vasıtalarını belirleyen, veri kayıt sisteminin kurulmasından ve yönetilmesinden sorumlu olan gerçek veya tüzel kişiyi ifade etmektedir. Bu kişilerin, Kanun’a uygun olarak uygulamalar ve ilkeler belirlemek yönünde sorumlulukları vardır. Şirketin iş süreçlerinde kullanılan tüm kişisel verilere ilişkin veri sorumlusu ilgili Şirket olmaktadır.

Data Officer: *refers to the real or legal person responsible for identifying the purposes and means of personal data processing and installing and managing data registry system. These persons have responsibilities such as identifying applications and principles in compliance with the Law. Data responsible person with regard to all personal data used in the business processes of the Company is the relevant Company.*

Veri İşleyen: Bir veri sorumlusu tarafından verilen yetkiye dayanarak ve onun adına veri işleyen herhangi bir kişidir. Veri sorumlusunun çalışanlar bu tanımın dışındadır, ancak uygulanabilir olması halinde, Şirket adına kişisel veri işleyen tedarikçiler, iş ortakları ve diğer üçüncü kişiler bu tanıma dâhil edilebilir.

Data Processor: refers to any person processing data based on the power granted by a data owner or on its behalf. Employees of data supervisor are outside of this definition; however, if applicable, the suppliers processing personal data on behalf of the Company, business partners and other third parties can be included in this definition.

Veri İşleme / İşleme: Veri kullanımına ilişkin her türlü aktiviteyi kapsamaktadır. Verinin elde edilmesi, kaydedilmesi ya da tutulmasını, ya da veriyi düzenlenme, değiştirme, geri alma, kullanma, açıklama, silme ya da yok etme de dâhil olmak üzere veri üzerinde yürütülen bir veya bir takım işlemleri içerir. Verinin üçüncü kişilere aktarılması da verinin işlenmesi anlamına gelmektedir.

Data Processing/Processing: It covers all kinds of activities relating to data use. It includes one or a set of procedures executed over the data including acquisition, recording or retention of data or data editing, changing, retrieval, use, description, erasing or destruction. Transfer of data to third parties refers to the processing of data.

POLİTİKANIN AMACI PURPOSE OF POLICY

İşbu Politika ile amaçlanan, Şirket tarafından Kanun'a uyum için gerekli düzenlemelerin Şirket bünyesinde benimsenmesinin sağlanması, uygulanacak politikaların düzenlenmesi ve iştirakler arasında bir birliğin oluşturulmasıdır. Bu bağlamda Politika, Kanun ve ilgili mevzuat tarafından konulan kuralların Şirket tarafından nasıl uygulandığına / uygulayacağına ilişkin temel ve tüm iş birimleri için geçerli kurallar ve ilkelerin belirlenmesidir.

It is aimed with this Policy to ensure adoption of requirement arrangements within the Company for compliance with the Law by the Company, to arrange applicable policies and form a union between the affiliates. In this context, it is to set forth applicable rules and principles for key and all business units relating to how the rules imposed by the Policy, Law and relevant legislation have been applied/shall be applied.

Şirket, tüm iç süreçlerini Politika'ya uygun hale getirmelidir. Politika'ya uyum için gerekli düzenlemeler yapılmalı ve belirli aralıklara Politika'ya uyum konusunda, denetim mekanizmalarını işleterek Politika'ya uyumun devamlılığı sağlanmalıdır. Konu ile ilgili tüm çalışanların Politika'ya uyumunu teyit edecek ve değişiklikler hakkında tüm ilgililerin bilgilendirilmesi gerekecektir. Değişen ve yenilenen süreçlere, en kısa sürede uyum gösterilmesi için şirket içi eğitimler düzenlenmeli ve konu ile ilgili tüm çalışanlar nezdinde tüm sürecin Kanun'a uygun yürütülmelidir.

The Company should adapt all internal processes in compliance with the Policy. Necessary arrangements should be made for compliance with the Policy and continuity of compliance with the Policy should be ensured by operating inspection mechanisms in the issue of compliance with the Policy in specific intervals. All employees relating to the subject should verify their compliance with the Policy and all relevant persons should be informed regarding the changes. In-house training should be arranged for showing compliance with the changed and renewed processes within the shortest time possible and entire process within all employees should be executed in compliance with the Law relating to the issue.

Bu Politika ile Şirket'in Kanun ve ilgili mevzuat kapsamında gerekli idari yapı, süreç ve prosedürlerin oluşturulup, Kişisel Verilerin güvenliği ve korunması hususunda gerekli teknik ve idari önlemlerin alınması sağlanarak, Kişisel Verilerin Kanun'a uyumlu şekilde işlenmesinin ve tutulmasının içselleştirilmesi, çalışanlar ve tüm iş ortaklarında gerekli farkındalığın yaratılarak, Kanun'a uyum sağlanmalıdır.

With this Policy, required administrative structure, process and procedures should be formed within the Law and the relevant legislation of the Company and it should be ensured that required technical and administrative measures are taken in the issue of safety and protection of personal data and processing and retention of claimant of precautionary attachment in compliance with the Law should be internalized and required awareness should be raised in all employees and all business partners and compliance with the Law should be ensured.

I. KİŞİSEL VERİLERİN İŞLENMESİNE İLİŞKİN İLKELER

I. PRINCIPLES RELATING TO PROCESSING PERSONAL DATA

Şirket, Kişisel Verilerin Kanun ve ilgili mevzuatta öngörülen genel ilkelere uygun olarak işlenmesi amaçlanmalıdır. Bu kapsamda, Şirket tarafından Kişisel Veriler;

It should be aimed by the Company to process the personal data in compliance with the general principles stipulated in the relevant legislation and the Personal Data Law. In this context, personal data by the company

a) Hukuka ve iyi niyete uygun olarak işlenmelidir:

a) should be processed in accordance with the law and in good faith:

- Bu ilkenin amacı Kişisel Verinin işlenmesi önlemek değil, Kişisel Verilerin işlenmesinin dürüstlük kurallarına ve hukuka uygun, Veri İlgisinin haklarını olumsuz şekilde etkilemeyecek şekilde yapıldığından emin olmaktır.

- Purpose of this policy is to ensure that processing of personal data is performed in compliance with integrity rules and law and in a manner that shall not adversely

impact the right of the data relevant person other than preventing processing personal data.

- Veri Sahibine, Veri Sorumlusunun kim olduđu, verinin Őirket tarafından hangi amala iŐleneceđi, verinin aıklanabileceđi veya aktarılabilceđi kiŐilerin kimliđi ve bu veri sahibinin hakları sylenmelidir.

- *Data Owner should be informed of the fact that who the Data Supervisor is, with what purpose the data is to be processed by the Company, the identity of the person to whom data is to be disclosed or can be transferred and the rights of this data owner.*

- KiŐisel Verinin hukuka uygun olarak iŐlenebilmesi iin bir takım Őartların sađlanması gerekir. Bunlar, diđerlerinin yanı sıra, Veri Sahibinin KiŐisel Verilerinin iŐlenmesine rıza gstermiŐ olması ya da iŐlemenin Veri Sorumlusunun veya verinin aklandıđı üçüncü kiŐinin meŐru menfaati kapsamında gerekli olması gibi gereklilikleri ierebilir. Bazı durumlarda Veri Sahibinin ilgili verinin iŐlenmesine iliŐkin aık onay vermesi gerekebilir.

- *A set of requirements should be met for processing personal data in compliance with the law. These, inter alia, may incorporate the requirements indicating that Data Owner should give its consent to data processing or processing is required within the scope of legitimate interest of third parties to which data is to be disclosed or Data Supervisor. In some cases, Data Owner should give express consent relating to processing of the relevant data.*

- KiŐisel Veriler, Veri Sahibinin aık rızası halinde iŐleme hari olarak, ancak iŐlemenin kanunlarda aıka öngörölmüŐ olması; fiili imkansızlık nedeniyle rızasını aıklayamayacak durumunda bulunan veya rızasına hukuki geçerlilik tanınmayan kiŐinin kendisinin ya da bir baŐkasının hayatı veya beden bütünlüđünün korunması iin zorunlu olması; bir szleşmenin kurulması veya ifasıyla doğrudan doğruya ilgili olması kaydıyla, szleşmenin taraflarına ait kiŐisel verilerin iŐlenmesinin gerekli olması; iŐlemenin veri sorumlusunun hukuki yükümlölüđünü yerine getirebilmesi iin zorunlu olması; iŐlenen verinin ilgili kiŐinin kendisi tarafından alenileŐtirilmiŐ olması; iŐlemenin bir hakkın tesisi, kullanılması veya korunması iin zorunlu olması; ilgili kiŐinin temel hak ve özgürlüklerine zarar vermemek kaydıyla, iŐlemenin veri sorumlusunun meŐru menfaatleri iin zorunlu olması hallerinden birinin varlıđı halinde iŐlenecektir. Ancak KiŐisel Verilerin iŐlenmesine iliŐkin burada sınırlı olarak sayılan istisnalar kapsamında iŐlenen verilerin Veri İlgililerine, Kanun'un 16. Maddesi uyarınca öngörölen Aydınlatma Yükümlölüđü'nü kapsayacak Őekilde bilgilendirme yapılmalı, sz konusu bilgilendirme ile KiŐisel Verilerin Őirket tarafından iŐbu Politika uyarınca iŐlendiđi konusunda bilgi verilmeli ve verilerin Kanun, ilgili mevzuat ve iŐbu Politika'ya uygun olarak iŐlendiđi teyit edilmelidir.

- Provided that the processing transaction is expressly stipulated in the laws except for the transaction if the Data Owner gives an express consent, if it is mandatory for life or body of the person or another person is to be protected, to which legal validity is recognized to its consent or with incapacity to disclose its consent; it is directly in relation to establishment or performance of the contract directly, processing is mandatory in order for fulfilling legal obligation of data supervisor, processed data is made public by the relevant person, a processing is mandatory to establish, use or protect one right of processing; it shall not prejudice the fundamental rights and freedoms of the relevant person, in case of availability of one of the mandatory cases for legal interest of data supervisor. However, information should be provided in a manner that shall cover disclosure requirement provided as per Article 16 of the Law to the Data Relevant Persons in regard to the data processed within the scope of the exceptions referred limited to here in relation to the processing of personal data and the information should be provided in the issue indicating that the personal data is processed as per this Policy with the said information and the data should be verified that they are processed in compliance with the Law, the relevant legislation and this Policy.

- Şirket, bu çerçevede, Kanun'daki düzenlemelere uyum için gerekli süreçleri oluşturmalıdır.

- The Company, within this framework, should create required processes for regulatory compliance in the Law.

b) Belirli, açık ve meşru amaçlar için işlenmelidir:

b) should be processed for specific, clear and legitimate purposes:

- Kişisel Veri, verinin ilk toplandığı sırada Veri Sahibine bildirilen belirli amaçlar çerçevesinde ya da Kanun tarafından özellikle izin verilen herhangi başka bir amaçla işlenebilir. Bu, Kişisel Verinin belirli bir amaç için toplanıp, sonradan başka bir amaç için kullanılmayacağı anlamına gelir. Eğer Kişisel Verinin işlenme amacının değiştirilmesi zorunlu hale gelirse, Kişisel Veri işlenmeden önce veri sahibinin söz konusu yeni işleme amacından haberdar edilmesi gerekir.

- Personal data may be processed for another purpose permitted specifically by the Law or within the framework of specific purposes notified to the Data Owner during the first collection of data. This means that Personal data is collected for a specific purpose and may not be used for another purpose. If it becomes necessary to change the purpose of processing the personal data, the data owner should be informed of the purpose of new processing in question prior to processing personal data.

c) Sınırlı, ölçülü ve amaç için gerekli şekilde işlenmelidir:

c) should be processed as required for purpose and in limited, moderate manner:

- Kişisel veri, sadece Veri Sahibine bildirilen belirli amacın gerektirdiği ölçüde toplanmalıdır. Bu amaç için gerekli olmayan herhangi bir verinin toplanmaması gerekir. Tüm çalışanlar gerekli olmayan kişisel verileri almaktan kaçınmalıdır. Tedarikçilerle/üçüncü kişilerle imzalanan sözleşmeler de bu kuralı yürürlüğe koyan mekanizmalar içermelidir.

- Personal data should be collected to the extent required by specific purpose notified to the Data Owner only. Any data not required for this purpose may be required to not to be collected. All employees should avoid receiving personal data that is not necessary. The contracts executed with suppliers/third parties should include the mechanisms putting this rule into force.

d) Doğru ve gerektiğinde güncel olmalıdır:

d) should be accurate and up to date when necessary:

- Veri Sahiplerinin verilerini güncellemeleri için olanaklar tanınmalı ve bu olanaklar konusunda Veri Sahipleri bilgilendirilmelidir. Kişisel verilerin alınması sırasında, güncelleme süreçlerine ilişkin Veri Sahiplerine bilgi verilmelidir. Çalışanlar tarafından da belirli aralıklarla verilerin güncelliği teyit edilmeli ve güncel olmayan veya güncel olarak işlenmesinde yarar görülmeyen tüm veriler, güncellenme imkânı söz konusu değil ise silinmeli ya da anonim hale getirilmelidir.

- Possibilities should be recognized for the Data Owners to update their date and the Data Owners should be informed in the issue of these possibilities. The Data Owner should be informed in relation to update processes during reception of personal data. Up to date condition of date should be periodically verified by employees and all data that is not useful for processing either in up to date or non-up to date condition should be erased or anonymized if there is no possibility of an update.

e) İlgili mevzuat uyarınca öngörölmüş süreden ya da veri toplama amacının zorunlu kıldığı süreden fazla tutulmamalı / saklanmamalı ve arşivlenmemelidir:

e) should not be kept/stored or archived more than the period obligated by the purpose of data collection or the period stipulated as per the relevant legislation:

- Kişisel Veri, amacın gerektirdiğinden daha uzun süre tutulmamalıdır. Başka bir deyişle, kişisel verilerin işlenmesi artık gerekli olmadığında veya ihtiyaç kalmadığında, kişisel veriler yok edilmeli ya da Şirket'in sistemlerinden silinmelidir

veya anonim hale getirilmelidir. Kişisel Verinin gelecekte kullanılması gerekebileceği varsayımı ile saklanmaması ve arşivlenmemesi gerekmektedir.

- Personal data should not be kept longer than required by its purpose. In other words, if the processing of personal data is no longer required or needed, personal data should be disposed of or should be erased from the systems of the Company or should be anonymized. Personal data should not be kept and archived with the assumption that it may be required to be re-used in the future.

- Her bir iş birimi, farklı türdeki Kişisel Verilerin işlenmesi için gerekli süreyi değerlendirmeli ve gerekli sürenin ne kadar olduğunu yazılı şekilde belirlemelidir. Bu süre, işlemin amacı gereğince iş biriminin veriyi tutmasını gerektiren süreyi aşmamalıdır.

- Each business unit should consider the required period for personal data personal data in different types and should designate how much the required period is in writing. This period should not exceed the period requiring the business unit to retain the data as per the purpose of the processing.

- Kişisel Verilerin saklanması, silinmesi, yok edilmesi ve anonim hale getirilmesine ilişkin politikalara ilişkin (V) başlığına bakınız.

- Refer to (V) title relating to the policies concerning storage, erasing, destruction and anonymization of personal data.

f) Veri Sahibinin haklarıyla uyumlu olarak işlenmelidir:

f) should be processed in compliance with the rights of the Data Owner:

- Veri Sahibini haklarına ve hukuki başvuru yollarına ilişkin (III) başlığına bakınız.

- Refer to (III) title in relation to the rights of the Data Owner and legal remedies.

g) Güvende tutulmalıdır:

g) should be kept safe:

- Veri Güvenliğine ilişkin Şirket politikalarının detaylarına ilişkin (IV) başlığına bakınız.

- Refer to (IV) title relating to the Company policy details concerning Data Security.

h) Yeterli korumaya sahip olmayan ülkelerde bulunan kişilere ya da organizasyonlara aktarılmamalıdır:

h) should not be transferred to the persons or organizations in the countries having insufficient protection:

- Şirket tarafından Kişisel Veriler, mümkün olduğu kadar yurtdışına aktarılmamalıdır. Arşivleme amacı ile Kişisel Verilerin tutulduğu, üçüncü kişilerin mülkiyetindeki serverlar dahi mümkün olduğu kadar Türkiye’de yer almalı ve güncel durumda verilerin yurtdışına aktarımı söz konusu olmamalıdır.

- *Personal Data should not be transferred abroad as far as possible by the Company. The servers that are retained for Personal data for archiving purpose and under the property of third parties should be located in Turkey as far as possible and the data should not be transferred abroad in up to date condition.*

- Ancak, Şirket politikaları gereği Kişisel Verilerin yurtdışına aktarılması veya yurtdışındaki serverlarda tutulmasının kararlaştırılması halinde, ancak KVKK hükümlerine uygun şekilde ve Kişisel Verileri Koruma Kurulu’nun (“Kurul”) belirleyeceği kurallar çerçevesinde yurt dışına aktarılmalıdır.

- *However, in cases it is agreed to retain personal data in servers abroad or to transfer abroad as per the policies of the Company, they may only be transferred abroad within the framework of the rules to be designated by Personal Data Protection Board ("Board") and in compliance with the provision of Personal Data Protection Law.*

- Kişisel Verilerin üçüncü kişilere aktarımına ilişkin (IV) başlığına bakınız.

- Refer to (IV) title relating to the transfer of personal data to third parties.

II. KİŞİSEL VERİ SAHİBİNİN HAKLARI

II. RIGHTS OF PERSONAL DATA OWNER

Kişisel Veri Sahipleri, Kanun’un 11. Maddesinde düzenlenen,
As set forth in Article 11 of the Law, the Personal Data Owners are entitled to

- i. Kişisel Verisinin işlenip işlenmediğini öğrenme,
Becoming aware of whether the personal data has been processed or not,

- i. Kişisel Veri işlenmişse, buna ilişkin bilgi talep etme, *Becoming aware of the purpose of personal data processing and whether or not the data has been used for the purpose provided,*
- ii. Kişisel Veri işleme amacını ve verilerin amaca uygun kullanılıp kullanılmadığını öğrenme,
- iii. *Requesting information regarding the personal data if they are processed,*
- iv. Kişisel Verilerin aktarıldığı üçüncü kişileri öğrenme ve *Becoming aware of the third parties to whom personal data is transferred and*
- v. Kişisel Veriler eksik ya da yanlış işlenmişse bunların düzeltilmesini isteme ve bunun Kişisel Verilerin aktarıldığı üçüncü kişilere bildirilmesini talep etme hakları ile

If personal data has been processed improperly or inaccurately, the right of requesting their correction and requesting them to be notified to the third parties to whom Personal data is transferred and

- vi. Kişisel Verilerin Kanun'a aykırı işlenmesi sebebiyle zarara uğranması durumunda tazminat talep etme haklarını haiz olup Şirket tarafından Veri Sahibinin talebi üzerine bu hakların yerine getirilmesi konusunda en kısa süre içerisinde aksiyon alınacak ve Veri Sahibine taleplerine ilişkin prosedür ile ilgili detaylı bilgi verilecektir.
- ii. *the rights of claiming compensation if Personal data is damaged due to processing in contradiction with the Law and the action shall be taken as soon as possible in the issue of fulfilling these rights upon the request of the Data Owner by the Company and the detailed information relating to the procedure regarding the requests shall be provided to the Data Owner.*



III. KİŞİSEL VERİLERİN GÜVENLİĞİ III. SECURITY OF PERSONAL DATA

Şirket, Kişisel Verilerin hukuka aykırı işlenmesini önlemek, Kişisel Verilere hukuka aykırı olarak erişilmesini önlemek ve Kişisel Verilerin muhafazasını sağlamak amaçlarıyla uygun güvenlik düzeyini temin etmeye yönelik gerekli her türlü teknik ve idari tedbirleri almakla yükümlüdür.

The Company is liable for adopting all kinds of technical and administrative measures required for procuring security level complying with the purposes for ensuring the preservation of Personal data and preventing the access the personal data in contradiction with the law and preventing personal data of personal data in contradiction with the law.

Şirket, hukuka aykırı ya da yetkisiz Kişisel Veri işlenmesine veya Kişisel Verinin bir kaza sonucu kaybı ya da zarar görmesine karşı uygun güvenlik önlemlerinin alındığından emin olmalıdır. Bu tür zararlara uğramaları durumunda Veri Sahipleri, dava yolu ile tazminat talebinde bulunabilirler.

The Company should make sure that appropriate safety measures have been taken against the loss or damage of personal data as a result of an accident or processing authorized personal data or that is in contradiction with the law. If they suffer such losses, Data Owners can request compensation via lawsuit.

Kanun, Kişisel Verilerin toplanma anından yok edilme anına kadar güvenliğinin sağlanabilmesi için, Şirket'in bir takım idari ve teknik önlemler almasını zorunlu kılmaktadır.

The Law stipulates that the Company should adopt a set of administrative and technical measures for ensuring the security of personal data from their collection time to destruction time.

Veri güvenliğinin sağlanması, aşağıda tanımlandığı üzere, kişisel verinin gizliliğinin, bütünlüğünün ve erişiminin garanti altına alınması anlamına gelmektedir.

Ensuring data security refers to securing personal data confidentiality, integrity and access as defined below.

- i. Gizlilik, sadece veriyi kullanmaya yetkili kişilerin veriye erişmesi anlamına gelmektedir.

Confidentiality refers to accessing data by only persons authorized to use the data.



- ii. Bütünlük, kişisel verinin doğru olması ve işleme amacına uygun olması anlamına gelmektedir.
Integrity refers to correct personal data and fit for processing purpose.
- iii. Erişim, yetkili kullanıcıların, yetkilendirilmiş oldukları amaç çerçevesinde ihtiyaç duymaları halinde, veriye erişebilmeleri anlamına gelmektedir.
Access refers to the ability to access the data if needed within the scope of the purpose authorized by the authorized users.

Kişisel Verilere ilişkin güvenlik prosedürleri, veri güvenliğine ilişkin teknik anlamda yetkin Şirket bünyesi veya Şirket tarafından bu konu ile ilgili teknik yardım talep edilen firmanın Bilişim Teknolojileri ("BT", "IT") birimine danışılarak yürürlüğe konulmalıdır.

Security procedures relating to personal data should be put into force by consulting the Department of Information Technologies ("IT") of the firm from which technical assistance is requested in relation to this issue by the Company or within the competent Company in the technical sense in relation to the data security.

Şirket'in hâlihazırdaki uygulamalarına uyumlu olarak her bir iş biriminin erişim yetkileri, ilgili iş birimi bakımından gerektiği ölçüde sınırlandırılmalıdır. İlgili sınırlandırmalar, Şirket nezdinde düzenli aralıklarla gözden geçirilmeli ve Kişisel Verilere erişim yalnızca zorunlu olduğu ölçüde söz konusu olabilmelidir.

Access authorities of each business unit in compliance with the present applications of the Company should be limited to the extent required in terms of the relevant business unit. Relevant limitations should be periodically revised within the Company and personal data may only be accessed in case of obligatory conditions.

Şirket'in tüm çalışanları, veri güvenliğine ilişkin belirlenecek prosedürler çerçevesinde bilgilendirilmeli ve eğitilmelidir. Bu kapsamda, Kişisel Verilere erişmek üzerine şifre ile giriş yapılan sistemlere ilişkin şifreler, herhangi bir üçüncü kişiye veya yetkisiz çalışana açıklanmamalıdır. Kişisel Verilere erişme yetkisi verilen kullanıcılar, uygulanabilir olması durumunda, bireysel ekranlarının yakınından geçenlere gizli bilgilerin gösterilmediğinden ve ekranlarının başında olmadıkları zaman bilgisayar oturumlarını kapattıklarından emin olmalıdırlar.

All employees of the Company should be informed and trained within the framework of the procedures to be designated in relation to the data security. Within this context, the passwords relating to the systems logged in with the

password for accessing Personal data should not be disclosed to any third parties or unauthorized employee. If applicable, the users that have been allowed with access authority to the personal data should ensure that confidential information is not shown to those passing from the vicinity of the individual screens and those should make sure that they have logged out from their sessions when they are not in front of their screens.

Şirket nezdinde tutulan Kişisel Veriler dahil tüm verilerin güvenliği için gereken teknik önlemler alınmalı, mevcut güvenlik sistemleri, virüs koruma programları ve ileti gönderilerine ilişkin koruma sistemleri periyodik olarak denetlenmeli, tüm bu sistemlerin en güncel sürümleri yürürlüğe konulmalıdır. Bu konuda, teknolojik gelişmeler takip edilmeli ve ortaya çıkabilecek risklere en kısa sürede müdahale edecek teknik ekip ve sistem tahsis edilmelidir.

Technical measures required for all data security including Personal data retained within the Company should be taken; protection systems relating to existing safety systems, virus protection programs and message transmission should be periodically inspected and the most recent update versions of these systems should be put into force. In this regard, technological advancements should be followed up and technical team and system shall be allocated in a manner that the resulting risk is intervened as soon as possible.

Yukarıdakilere ek olarak, tüm Şirket çalışanları, işlenen Kişisel Verilerin kanuni olmayan yollarla başkaları tarafından elde edilmesi ve/veya Kişisel Verilerin güvenliğine ilişkin herhangi bir riskin söz konusu olması hâlinde derhal gereken önlemlerin koordinasyonu ve uygulanabilir olması halinde bu durumun en kısa sürede ilgili Veri Sahibine ve Kurula bildirilmesi için [Şirket'in KVK Komitesi] birimine bilgi vermelidir.

In cases in addition to the foregoing, where processed personal data of entire Company employees is acquired by the others with non-legal means of Data and/or there is any risk relating to security of personal data, Personal Data Protection Committee of the company should be informed for notifying to the relevant Data Owner and Board as far as possible if applicable and coordination of measures required immediately if this risk is in question.

Uygulanabilir olması halinde, Kişisel Verilerin hukuka uygun olarak aktarıldığı mevcut üçüncü kişiler ile yapılan sözleşmeler, hâlihazırdaki gizlilik yükümlülüklerine ek olarak, Kişisel Verilerin aktarıldığı kişilerin, Kişisel Verilerin korunması amacıyla gerekli güvenlik tedbirlerinin alınacağı ve kendi işletmelerinde / kurumlarında / kuruluşlarında bu tedbirlere uyulmasını sağlayacağını temin üzere değiştirilmelidir. Şirket'in gerektirdiği güvenlik önlemlerini sağlamayan ve verilerin gizliliği, bütünlüğü ve erişimine ilişkin Kanun'un gerekliliklerini yerine getirmeyen üçüncü kişilere hiçbir surette Kişisel Veri aktarılmamalıdır.

If applicable, the contract executed with the present third parties to whom Personal data is transferred in compliance with the Law should be amended so as to procure that required safety measures are taken for protecting the personal data of the persons to whom Personal data is transferred in addition to the available confidentiality obligations and to ensure that these measures are followed in its own enterprises/institutions/organizations. Personal Data should under no circumstances be transferred to the third parties failing to fulfil the requirements of the Law with respect to confidentiality, integrity and access and failing to security measures required by the Company.

IV. KİŞİSEL VERİLERİN ÜÇÜNCÜ KİŞİLERE AKTARILMASI **IV. TRANSFERRING PERSONAL DATA TO THIRD PARTIES**

Kişisel Verilerin yurtiçindeki üçüncü kişilere aktarılabilmesi, Kişisel Verilerin işleme amaçları ile Veri Sahipleri ile akdedilen sözleşmelerin ifası için zorunlu olması ve Şirket'in meşru menfaatleri gerektirdiği ölçüde Kanun'un öngördüğü şartlara uygun olarak gerçekleştirilmelidir. Kişisel Verilerin işleme amaçları dışında başka bir amaçla veri aktarımı yapılmamalıdır. Ancak her ne kadar İşlemenin, rıza alınmasını gerektiren istisnaları kapsamında değerlendirilse de elde edilecek olan yeni Veri Sahiplerinin Kişisel Verilerinin Şirket'in gerektirdiği güvenlik önlemlerini alan iş ortaklarına aktarılması için ilgili Veri Sahibinin açık rızasının alınması sağlanmalıdır. Şirket, iş ortaklarının seçiminde kişisel verilerin gizliliğine ilişkin hususlarda ön inceleme yapmalı ve onlarla yapacağı sözleşmelerde Kişisel Verilerin güvenliği ve gizliliğine ilişkin Kanun'un gerekliliklerini tatmin edecek hükümlere yer verilmesini sağlamalı, devam eden sözleşmelerde ise buna ilişkin ek sözleşme düzenlenmelidir.

Transferring personal data to domestic third parties should be performed in compliance with the requirements stipulated by the Law to the extent required by legitimate interests of the Company and performance of the contracts executed with the Data Owner is obligatory for the purpose of processing personal data. No data transfer should be performed for another purpose other than the purposes of processing personal data. However, no matter of processing is considered within the scope of the Project exceptions requiring obtaining consent; it should be ensured that explicit consent of the relevant Data Owner should be obtained for transferring Personal data of new Data Owner to be obtained for the safety measures required by the Company. Preliminary examination should be conducted in the matters in relation to the confidentiality of personal data in selection of business partners by the Company and it should be ensured that the provisions that



shall satisfy the requirements of the Law exist in relation to the security and confidentiality of the Personal data and additional contracts should be arranged in relation to this in the continuing contracts.

Şirket tarafından Kişisel Veriler, mümkün olduğu kadar yurtdışına aktarılmamalıdır. Arşivleme amacı ile Kişisel Verilerin tutulduğu, üçüncü kişilerin mülkiyetindeki serverlar dahi Türkiye’de yer almalı ve güncel durumda verilerin yurtdışına aktarımı söz konusu olmamalıdır. Ancak, Şirket politikaları gereği Kişisel Verilerin yurtdışına aktarılması veya yurtdışındaki serverlarda tutulmasının gerekli olması halinde, alınmamış ise Veri İlgilisinin ilgili Şirket tarafından açık rızası alınmalı ve veri, kural olarak, Kurul’un belirleyeceği yeterli korumanın bulunduğu ülkeler dışında bir ülkeye aktarılmamalıdır.

- Personal Data should not be transferred abroad as far as possible by the Company. The servers that are retained for Personal data for archiving purpose and under the property of third parties should be located in Turkey and the data should not be transferred abroad in up to date condition. However, if it is necessary to retain personal data in servers abroad or to transfer abroad as per the policies of the Company, if obtained, express consent of the Data Relevant Person should be obtained by the relevant Company and the data, as a rule, should not be transferred to the country other than the countries where sufficient protection is available, as laid down by the Board.

Kişisel Veriler, uygulanabilir olması durumunda, ancak Şirket ve ilgili ülkede veri sorumlusu olacak gerçek ve/veya tüzel kişi tarafından yeterli korumanın bulunduğu yazılı olarak taahhüt edilmek ve Kurul’un veri transferine izni alınmak kaydıyla yeterli korumanın olmadığı yabancı ülkelere de aktarılabilir.

Personal data can also be transferred to the foreign countries where no sufficient protection is available provided that it is in writing committed that there is sufficient protection by real and/or legal person that shall be data supervisor in the Company and relevant country and consent for data transfer of the Board is obtained.

Bu bağlamda, Şirket tarafından Kanun’un 8. ve 9. Maddesinde öngörülen düzenlemelere uygun hareket etmeye yönelik gerekli süreçler tasarlanmalıdır. Politika’yı onaylayan Veri Sahipleri, işbu Politika’da belirtilen hususlara tabi olmak üzere, Kişisel Verilerinin, işlenmesinin gerektirdiği amaçlar ve arşivleme amacı ile sınırlı olarak, kanun ve yargı kararları ile idari kararlar dâhil kamu kurum ve kuruluşlarının ilgili mevzuatta düzenlenen hakları çerçevesinde bilgi ve belge talep ettiği hallerde Kişisel Verilerin aktarılacağı istisnası saklı kalmak kaydıyla, Şirket ve/veya üçüncü kişi iş ortakları, hizmet/destek/danışmanlık alınan ya da işbirliği yapılan ya da proje/program/finansman ortağı olunan kamu/özel

kurum ve kuruluşlar, tedarikçiler, Şirket'in ortakları, şirket yetkilileri, bankalar, fonlar ve sair 3. kişi ya da kuruluşlar ile paylaşılmasına açık şekilde rıza gösterdiği belirtilmelidir.

In this context, required processes in regard to acting in compliance with the arrangements stipulated in Article 8 and 9 of the Law should be designed by the Company. In cases where Data Owner approving the Policy requests information and documents within the framework of the rights regulated in the relevant legislation of public institution and organization including the administrative decision with the law and judicial decision limited to the archiving purpose and the purposes required by the processing of Personal data as subject to the consideration specified in this Policy, it should be indicated that the exchanging the personal data with Company and/or third party business partners, service/support/consultancy received or collaborated or project/program/financing partnered public/private institutions and organizations, suppliers, partners of the Company, company authorities and banks, funds and other 3rd party or organizations are expressly consented.

Şirket, tüm Veri İlgililerine aydınlatma yükümlülüğünü yerine getirmeli ve veri aktarımına ilişkin Veri İlgililerinin yazılı rızalarını almalıdır.

The Company should fulfil all disclosure statements to the Data Relevant Persons and should obtain the written consent of the Data Supervisor in relation to data transfer.

V. KİŞİSEL VERİLERİN SİLİNMESİ, YOK EDİLMESİ VE ANONİMLEŞTİRİLMESİ PROSEDÜRLERİ **V. ERASING, DESTRUCTION AND ANONYMIZATION PROCEDURES OF PERSONAL DATA**

Kişisel Verilerin Silinmesi ve Yok Edilmesi Prosedürü **Erasing and Destruction Procedure of Personal Data**

Şirket, Kanun'a uygun şekilde, işlenmesini gerektiren sebeplerin ortadan kalkması hâlinde, ilgili kanun ve mevzuatta öngörülen asgari saklama sürelerine riayet etmek koşulu ile Kişisel Verileri re'sen veya ilgili kişinin talebi üzerine silemeli veya yok etmelidir. Silme veya yok etme sırasında kullanılacak teknikler;

The Company should erase or destroy the personal data upon the request of the relevant person or ex officio provided that it shall abide by the minimum storage periods stipulated in the relevant law and legislation if the reasons requiring processing in compliance with the Law vanish. Techniques to be used during erasing or destruction;

1- Fiziksel Olarak Yok Edilebilir

1- Physically Destructible

Kişisel veriler herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla da işlenebilmektedir. Bu tür veriler silinirken/yok edilirken kişisel verinin sonradan kullanılmayacak biçimde fiziksel olarak yok edilmesi sistemi uygulanmalıdır.

Personal data can be processed with non-automatic means provided that they shall be a part of any data registry system. The system of physically destroying the personal data in a manner that it shall not be used then while erasing/destroying such data should be applied.

2- Yazılımdan Güvenli Olarak Silinebilir

2 - Safely Erasable from Software

Tamamen veya kısmen otomatik olan yollarla işlenen ve dijital ortamlarda muhafaza edilen veriler silinirken/yok edilirken; bir daha kurtarılamayacak biçimde verinin ilgili yazılımdan silinmesine ilişkin yöntemler kullanılmalıdır.

The methods in regard to erasing the data from the relevant software in a manner that shall not be restored again while erasing/destroying the data stored in digital environments and processed with full or partial automatic means should be used.

Kişisel Verileri Anonim Hale Getirme Prosedürü

Anonymization Procedure of Personal data

Kişisel verilerin anonimleştirilmesi, kişisel verilerin başka verilerle eşleştirilerek dahi hiçbir surette kimliği belirli veya belirlenebilir bir gerçek kişiyle ilişkilendirilemeyecek hâle getirilmesini ifade eder.

Anonymization of personal data refers to making personal data unlikely to be associated with any identifiable real person in any way even when personal data is paired with other data.

Anonimleştirme için kullanılan Prosedürler *Procedures used for Anonymization*

Maskleme (Masking)

Veri maskleme ile kişisel verinin temel belirleyici bilgisini veri seti içerisinde çıkartılarak kişisel verinin anonim hale getirilmesi yöntemidir.

This is the method in which key determinant information of personal data is extracted from data set with data masking and personal data is anonymized.

Toplulaştırma (Aggregation)

Veri toplulaştırma yöntemi ile birçok veri toplulaştırılmakta ve kişisel veriler herhangi bir kişiyle ilişkilendirilemeyecek hale getirilmektedir.

Through data aggregation method, several data is aggregated and personal data is made in a manner that is not associated with any person.

Veri Türetme (Data Derivation)

Veri türetme yöntemi ile kişisel verinin içeriğinden daha genel bir içerik oluşturulmakta ve kişisel verinin herhangi bir kişiyle ilişkilendirilemeyecek hale getirilmesi sağlanmaktadır.

Through data derivation, more general content is created from the content of the personal data and it is ensured that personal data is made in a manner that is not associated with any person.

Veri Karma (Data Shuffling, Permutation)

Veri karma yöntemi ile kişisel veri seti içindeki değerlerinin karıştırılarak değerler ile kişiler arasındaki bağın kopartılması sağlanmaktadır.

Through data shuffling, bond between values and persons are broken down by mixing values in a personal data set.

Kişisel Verilerin, silinmesi, yok edilmesi ve anonim hale getirilmesi için asgari süreler, ilgili Kişisel Veriyi işleyen iş birimi tarafından belirlenecek ve Şirket'in tüm sistemleri, bu süreçlere uygun hale getirilmelidir. Yasal zorunluluktan daha uzun süre veri saklanması ilişkin Şirket'in Kişisel Veri işleme amaçları uyarınca bir karar alınması halinde, bu karar ve Kişisel Verilerinin ne kadar süre işleneceğine ilişkin Veri İlgililerine ayrıca bilgi verilmelidir. Her halde, Şirket, Kişisel Verilerin saklanması

ilişkin prosedürlerine ve veri işleme amaçlarına ilişkin aydınlatma yükümlülüğüne uygun davranmak zorundadır.

Minimum periods for erasing, destruction and anonymization of personal data shall be designated by the business unit processing the relevant Personal data and all systems of the Company should be made adaptable to these processes. In cases where a decision is taken as per the purposes of processing personal data of the Company in relation to the data storage periods longer than legal obligations, this decision and should be also informed to the Data Relevant Person in relation to how much the period is to be processed. In any case, the Company should act in compliance with the disclosure statement in regard to the personal data processing and procedures relating to storage of Personal data.

İlgili kanun ve mevzuat uyarınca saklanması için asgari sürelerin söz konusu olduğu verilere ilişkin bu sürelerin geçmesinden önce Veri İlgililerinden gelecek silme, yok etme veya anonim hale getirmeye ilişkin talepler, ilgili yasal zorunluluklar açıklanmak kaydıyla reddedilmelidir.

The requests for erasing, destroying or anonymizing to be received from the Data Relevant Person before passing to these periods in relation to the data where minimum periods are in question for storage of the same as per the relevant law and legislation should be rejected provided that legal obligations are disclosed herewith.

Kişisel verilerin saklanmasına ilişkin mevzuatta bir süre düzenlenmemişse, Kişisel Veriler Şirket'in veri işleme amacı uyarınca belirleyeceği, mevcut iş yapış, prosedür ve uygulamaları ve ticari yaşamının teamülleri uyarınca işlenmesini gerektiren süre kadar işlenmeli; daha sonra silinmeli, yok edilmeli veya anonim hale getirilmelidir.

No period is regulated in the legislation in regard to storage of personal data, the personal data should be processed up to the period requiring processing as per existing business performance, procedure and applications and commercial life practices to be designated by the purpose of data processing of the Company and then should be erased, destroyed or anonymized.

Kişisel verilerin işleme amacı, ilgili mevzuat ve Şirket'in belirlediği süreler sona erse dahi, kişisel veriler olası hukuki uyuşmazlıklarda delil teşkil etmesi veya kişisel veriye bağlı ilgili hakkın ileri sürülebilmesi veya savunmanın tesis edilmesi amacıyla (güncellikleri teyit ve temin edilmeden) yeniden olağan işlenmeleri söz konusu olmamak kaydıyla arşivlenebilecektir. Arşivleme sürelerinin tespitinde zamanaşımı süreleri dikkate alınmakla beraber, Şirket'in kendi tecrübeleri ve benzer veri gruplarına ilişkin önceki talepler ışığında zamanaşımı sürelerini aşan süreler belirlenmesi mümkün olabilecektir. Bu durumlarda, kişisel verilere (güncellikleri ve işlenmelerine ilişkin yeni bir açık rızanın alınması teyit ve temin edilmeden) hukuki uyuşmazlığın çözümü dışında herhangi bir başka amaçla erişilmeyecektir. Arşivleme

için belirlenecek süreler sonunda, arşivlenmesine karar verilen veriler dahi silinecek, yok edilecek ve anonim hale getirilecektir.

Purpose of processing of personal data Even if the periods designated by the relevant legislation and Company end, personal data can be archived provided that their processing ordinarily again is not in question for establishing the defence, claiming the relevant right connected to personal data or constituting evidence in potential legal conflicts (without up to date conditions are verified and provided). The statute of limitation periods are taken into account in the determination of archiving periods and it shall be possible to determine the periods exceeding the statute of limitation periods by considering the previous requests in relation to the experiences and similar data groups of the Company. In these cases, personal data may not be accessed with another purpose other than settlement of the legal dispute. (without verifying and providing obtaining a new express consent in relation to their being up to date and being processed) The data decided to be archived at the end of the periods to be designated for archiving shall be erased, destroyed and anonymized.

Şirket tarafından işlenebilen başlıca Kişisel Veriler ve bu verilerin başlıca işleme amaçları:

Key Personal data that can be processed by the Company and primary processing purposes of this data:

Gerçek Kişi Müşteri Verileri **Real Person Customer Data**

Her Şirket için geçerli olmamakla beraber, gerçek kişi müşterilere ilişkin ad, soyad, adres, e-mail, cep tel, ev tel, iş tel, doğum tarihi, T.C. kimlik no, cinsiyet, banka bilgileri, ebeveyn türü, medeni durum, meslek, evlilik tarihi, eş adı, eş doğum tarihi, eğitim durumu, okul adı, çocuk sayısı, üye olunan dernekler, takip edilen medya, sosyal medya, telefon markası, tuttuğu takım, araba markası, en sık girilen web sitesi, yurtiçi seyahat tercihi, yurtdışı seyahat tercihi, beden ölçüsü, ayakkabı ölçüsü gibi her Şirket'in kendi ihtiyacına göre çeşitlendirilebilen verilerdir.

This is the data that can be diversified according to the need of each Company like name, surname, address, e-mail, mobile phone, home phone, business phone, date of birth, TR ID No., gender, bank information, parent type, marital status, occupation, date of marriage, spouse's name, birth date of spouse, education status, school's name, number of children, subscribed associations, followed media, social media, telephone brand, favourite team, car brand, most frequently accessed web site, domestic travelling preference, foreign travelling preference, body size, shoe number etc. as not to be applicable for each Company.

Söz konusu Kişisel Veriler, işlenen her Kişisel Veriyi kapsamamakla beraber, satış tarihçesi oluşturmak, fatura oluşturmak, fatura kesmek, üyelik hesabını tanımlamak, basılı iletişim materyalleri iletmek, ürünü teslim etmek, e-fatura göndermek, newsletter göndermek, pazarlama iletişimi yapmak, müşteri analizi yapmak, müşteri sadakatini artırmak, özel üretim yapmak ve benzeri amaçlar ile sınırlı olarak işlenmektedir.

The said personal data does not cover each personal data so processed and is processed limited to the procedures of creating sales history, invoice, issuing invoice, defining membership account, communicating printed communication materials, delivering product, sending e-invoice, sending newsletter, performing marketing communication, performing customer analysis, increasing customer loyalty, performing special production and similar purposes.

Kurumsal Müşteriler, Tedarikçi ve Hizmet Sağlayıcıların Personellerine ve İmza Yetkililerine İlişkin Veriler

Data relating to Personnel and Authorized Signatories of Corporate Customers, Supplier and Service Suppliers

Her Şirket için geçerli olmamakla beraber, kurumsal müşterilerin, tedarikçilerin ve hizmet sağlayıcıların imza yetkililerine ve şahıs firmalarına ilişkin personel adı, personel soyadı, personel sicil no, personel t.c. kimlik no, personel boyu, personel kilosunu, personel cinsiyeti, personel bedeni; imzaya yetkili kişinin adı, soyadı, e-mail, T.C. kimlik no, banka bilgileri, şahıs firmalarına ilişkin diğer bilgiler ve benzeri verilerdir.

These are the information and similar data relating to personnel name, personnel surname, personnel registration no, TR ID No, personnel height, personnel weight, personnel gender, personnel size in regard to authorized signatories of corporate customers, suppliers and service providers as not to be applicable for each Company and name, surname, e-mail TR ID No, bank information and person firms of the persons authorized to sign.

Söz konusu Kişisel Veriler, işlenen her Kişisel Veriyi kapsamamakla beraber, toptan satış yapmak, satış tarihçesi oluşturmak, fatura oluşturmak, fatura kesmek, ürünü teslim etmek, e-fatura göndermek, newsletter göndermek, pazarlama iletişimi yapmak, müşteri analizi yapmak, cari hesap açmak, mutabakat yapmak, proje bazlı devlet teşviki almak ve benzeri amaçlar ile sınırlı olarak işlenmektedir. Bu kişilere Şirket nezdinde işlenen verilerin aktarılması da söz konusu olabilecek ve aktarmaya ilişkin prosedürlerin neler olabileceği (V) başlığı altında düzenlenmiştir.

The said personal data is processed as limited to the purposes of performing wholesale, creating sales history, creating invoice, issuing invoice, delivering product, sending e-

bill, sending newsletter, performing marketing communication, performing customer analysis, opening current account, performing reconciliation and getting project-based state incentive and similar purposes as it shall not cover each Personal data. The data processed within the Company to these persons can be transferred and what the procedures relating to the transfer can be are regulated under the title of (V).

Potansiyel Müşteri Verileri **Potential Customer Data**

Her Şirket için geçerli olmamakla beraber, Şirket'in potansiyel müşterilerine ilişkin ad, soyad, email, cinsiyet, cep tel, doğum tarihi, ev adresi, iş adresi, beden, evlilik tarihi ve benzeri Kişisel Veriler işlenebilir.

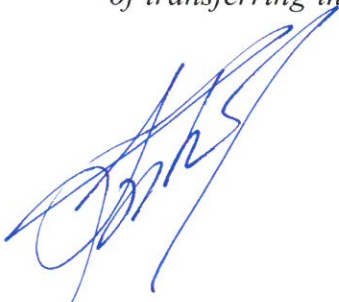
Name, surname, e-mail, gender, mobile phone, date of birth, home address, business address, size, date of marriage and similar personal data relating to the potential customers of the Company can be processed as not to be applicable for each Company.

Söz konusu Kişisel Veriler, işlenen her Kişisel Veriyi kapsamamakla beraber, hediye göndermek, etkinlik davetiyesi göndermek, newsletter göndermek, pazarlama iletişimi yapmak, analiz yapmak, yeni çıkan ürün hakkında bilgilendirmek ve benzeri amaçlar ile sınırlı olarak işlenmektedir.

The said personal data does not cover each processed Personal data and is limited to the purposes of sending gifts, sending event invitation, sending a newsletter, performing marketing communication, performing analysis, informing regarding newly released product and similar purposes.

Potansiyel müşterilere ilişkin veriler, söz konusu veriyi aktarmak konusunda verisinin Şirket tarafından yukarıda belirtilen amaçlar çerçevesinde işlenebileceğine ilişkin bilgilendirilmek kaydıyla, ilgili potansiyel müşterinin ilgili verinin üçüncü kişilere aktarımına rızası dâhilinde edinilmiş veriler olmaktadır. Potansiyel müşteriler ile ilk iletişimde, potansiyel müşteri, işbu Politika ve bu kapsamda işlenen verileri hakkında aydınlatma yükümlülüğü kapsamında bilgilendirilmeli ve itiraz / şikayeti üzerine söz konusu Kişisel Veri derhal silinmeli, yok edilmeli veya anonim hale getirilmelidir. Potansiyel müşteri ile müşteri ilişkisi kurulması halinde, bu kapsamda işlenen veriler de müşteri verilerine ilişkin prosedürlere tabi olmalıdır.

The data relating to potential customers is the data acquired within the consent for transfer of the relevant data of the relevant potential customer to the third parties provided that it shall be informed in relation to the processing of the data in the issue of transferring the said data within the framework of the purposes specified above by



the Company. In the first communication with the potential customers, the potential customer should be informed within the scope of the disclosure statement regarding the data processed within this context and this Policy and upon objection/complaint, the said personal data should be immediately erased, destroyed or anonymized. In case of establishing potential customer and customer relationship, the data processed within this scope should be subject to the procedures relating to the customer data.

Çalışan Verileri **Employee Data**

Her Şirket için geçerli olmamakla beraber, Şirket'in çalışanlarına ilişkin ad, soyad, doğum yeri, doğum tarihi, cep tel, e-mail, ikametgah adresi, ikametgahın durumu, ikamet edilen yapının yaşı, cinsiyet, maaş, medeni hali, eşinin adı, eşinin soyadı, eşinin iş durumu, mükellefle oturan veya mükellef tarafından bakılan çocukların durumu, çocuk sayısı, sicil no, t.c. kimlik no, sosyal güvenlik no, ayakkabı numarası, fotoğraf, acil durumda ulaşılabilecek kişinin adı soyadı, acil durumda ulaşılabilecek kişinin yakınlık derecesi, acil durumda ulaşılabilecek kişinin cep tel, eğitim bilgileri, özgeçmiş bilgileri, ikametgah belgesi, nüfus cüzdan sureti, diploma, çalışma belgesi, sabıka kaydı, kan grubu, askerlik belgesi, sağlık raporu, sigorta hizmet dökümü, SGK bildirme kaydı, iş sözleşmesi, not dökümü, referans mektubu, işe uyum anketi, performans formları, işten çıkış mülakat formu, mazeretli izin formu, yıllık izin formu, görev tanımları, sendikal bilgileri ve benzeri Kişisel Veriler işlenebilir.

Çalışanların sağlık verileri dâhil Özel Nitelikli Kişisel Verileri de, mevzuatın gerektirdiği ölçüde, İnsan Kaynakları iş birimi tarafından işlenebilir. Özel Nitelikli Kişisel Verilerin işlenmesine ilişkin (VII) başlığı altında düzenlenmiştir.

As not to be applicable for each Company, this data includes name, surname, place of birth, date of birth, mobile phone, e-mail residence address, status of residence, age of resided age, gender, wage, marital status, name of spouse, surname of spouse, employment status of spouse, status of children looked after by the tax payer or residing with tax payer, the number of children, registration number, TR ID No. social security no., shoe number, photograph, name and surname of the person to be called in case of emergency, relative degrees of the person to be called in case of emergency, mobile phone of the person to be called in case of emergency, education information, CV information, residence certificate, ID card copy, blood group, certificate of military status, health report, insurance service breakdown, Social Security Organization statement record, labour contract, note breakdown, reference letter, employment orientation questionnaire, performance forms, dismissal interview form, casual leave form, annual leave form, terms of references, union information and similar personal data.

Special Quality Personal Data including health data of employees can be processed by the business unit of Human Resources to the extent required by the legislation. Processing Special Quality Personal Data is regulated under the title of (VII).

Ayrıca, bir takım sağlık verileri iş yeri hekimi ve iş güvenliği uzmanları tarafından işlenebilir. İnsan Kaynakları ve işyeri hekimi tarafından işlenen sağlık verileri, 20 Ekim 2016 tarih ve 29863 sayılı Resmi Gazete’de yayınlanan Kişisel Verilerin İşlenmesi ve Mahremiyetinin Sağlanması Hakkında Yönetmelik ve diğer mevzuat uyarınca işlenebilir ve ilgili birimler haricinde hiçbir iş birimi ile paylaşılmamalıdır. Söz konusu verilere erişim en üst düzeyde sınırlandırılmalıdır. Bu veri grubuna ilişkin arşivleme amacıyla üçüncü kişiler ile paylaşımlar şifreleme sistemleri ile koruma altına alınmalı ve arşiv firması dâhil ilgili birimler dışında hiçbir kişinin sağlık verilerine erişimi söz konusu olmamalıdır. Üçüncü kişiler ile yapılan ilgili sözleşmeler, bu hususu teyit edecek şekilde revize edilmelidir. İşyeri hekimi tarafından işlenen verilerin arşivleme amacı için dahi olsa hiçbir üçüncü kişi ile paylaşımı söz konusu olmamalıdır. İşyeri hekimi tarafından ilgili sağlık verileri, Kişisel Sağlık Verilerinin İşlenmesi ve Mahremiyetinin Sağlanması Hakkında Yönetmelik uyarınca Sağlık Bakanlığı’nın belirleyeceği standartlar çerçevesinde sağlık verilerini Sağlık Bakanlığı nezdindeki Merkezi Sağlık Veri Sistemi’ne aktarılması gerekebilecektir.

In addition to this, a set of health data can be processed by the workplace physician and occupational safety specialists. Health data processed by the Human Resources and workplace physician can be processed as per the other applicable legislation and the Regulation on Personal Data Processing and Ensuring Confidentiality published in the Official Gazette dated 20 October 2016 and no. 29863 and should not be exchanged with any business unit except for the relevant units. Access to the said data should be limited at the top level. Exchanging with third parties for archiving relating to this data group should be protected with encryption systems and no person can access the health data other than the relevant units including archive firm. Contracts executed with the third parties should be revised in a manner that shall confirm this consideration. The data processed by the workplace physician should not be exchanged with third parties even for archiving purpose. Relevant health data by the workplace physician can be needed to be transferred to Central Health Data System within the Ministry of Health regarding the health data within the framework of the standards to be designated by the Ministry of Health as per the Regulation on Personal Data Processing and Ensuring Confidentiality.

Söz konusu Kişisel Veriler, işlenen her Kişisel Veriyi kapsamamakla beraber, personel kaydı açmak, atölyelerde performans ölçümü yapmak, personel maaşını ödemek, proje için devlet teşviki almak, işe giriş-çıkış saatlerini kaydetmek, bilgi güncellemek, çalışanın sigorta bildirimini yapmak, analiz yapmak, çalışanın performansını değerlendirmek, çıkış değerlendirmesi yapmak, izin almak, avans talebi işletmek ve benzeri amaçlar ile sınırlı olarak çalışanların rızası ve muvafakati dâhilinde işlenmelidir.

The said personal data does not cover each processed personal data and they should be processed within the consent and approval of the employees as limited to the purposes of opening personnel record, performing performance measurement in workshops, paying personnel wage, obtaining state incentive for project, recording employment starting-ending hours, updating information, performing insurance notification of employee, performing analysis, evaluating employee performance, performing exit evaluation, having leave, accruing advance request and similar purposes.

Çalışan verilerinin işlenmesi ve çalışanların özlük dosyaları İnsan Kaynakları birimi tarafından saklanmalı ve işlenmelidir. İnsan Kaynakları birimi tarafından işlenen veriler ile sınırlı olarak tüm çalışanlar, işbu Politika'nın kabul edilmesiyle mevcut sisteme ve Kişisel Verilerinin bordrosuna kayıtlı olduğu Şirket İnsan Kaynakları birimi tarafından işlenmesine rıza göstermelidir.

Processing employee data and personal files of employees should be stored and operated by the Human Resources Department. All employees as limited to the data processed by Human Resources Department should give their consent for their data to be processed by Human Resources Department of the Company registered to the payroll of Personal Data and existing system after the adoption of this Policy.

Çalışan Adayı Verileri **Employee Candidate Data**

Her Şirket için geçerli olmamakla beraber, Şirket'e çalışmak için başvuran adaylara ilişkin ad, soyad, anne adı, baba adı, cinsiyet, doğum yeri, doğum tarihi, askerlik durumu, medeni hali, eş adı, eş soyadı, çocuk sayısı, ikametgah adresi, ev telefonu, iş telefonu, cep telefonu, e-mail, acil durumda ulaşılabilecek kişinin adı soyadı, acil durumda ulaşılabilecek kişinin yakınlık derecesi, acil durumda ulaşılabilecek kişinin cep telefonu, acil durumda ulaşılabilecek kişinin ev telefonu, acil durumda ulaşılabilecek kişinin iş telefonu, özgeçmiş bilgileri, eğitim bilgileri, yabancı dil düzeyi, katıldığı staj, kurs ve seminerler, iş tecrübesi, şahsi bilgiler, referans veren kişinin adı, referans veren kişinin soyadı, referans veren kişinin çalıştığı yer/görevi, referans veren kişinin cep telefonu ve benzeri Kişisel Veriler işlenebilir.

As not to be applicable for each Company, name, surname, mother's name, father's name, gender, place of birth, date of birth, military service status, marital status, spouse name, spouse surname, the number of children, residence address, home telephone, business telephone, mobile phone, e-mail, name of the person to be called in case of emergency, relative degree of the person to be called in case of emergency, mobile phone of the person to be called in case of emergency, home phone of the person to be called in case of emergency, business phone of the person to be called in case of emergency, CV information, education information, foreign language level, participated apprenticeship, course and seminars, employment experience, personal

information, name of the person referencing, surname of the person referencing, employed place/position of the person referencing, mobile phone of the person referencing and similar Personal data.

Söz konusu Kişisel Veriler, işlenen her Kişisel Veriyi kapsamamakla beraber, uygun çalışan adayını işe almak amacıyla sınırlı olarak işlenebilir. Hizmet sözleşmesi ilişkisinin kurulması ile birlikte bu kapsamda işlenen veriler de çalışan verilerine ilişkin prosedür ve süreçlere tabi olacaktır.

The said personal data does not cover each processed personal data and may be processed as limited to for employing appropriately employed candidate. The data processed within this scope upon establishing a relationship of service contract shall be subject to the procedures and processes relating to the employee data.

Ödeme Araçlarına İlişkin Veriler **Data relating to Payment Instruments**

Her Şirket için geçerli olmamakla beraber, toptan satışlar ve benzeri faaliyetlere ilişkin mail order yöntemi ile ödeme gerçekleştirebilme olanağı tanınması için adı/unvanı, soyadı, kart sahibinin adı, kart sahibinin soyadı, kart sahibinin T.C. kimlik numarası, banka adı ve kart türü ile kredi kartı bilgileri ve benzeri Kişisel Veriler işlenebilir.

As not to be applicable for each Company, name/title, surname, card holder name, card holder surname, card holder TR ID Number, bank name and card type and credit card information and similar Personal data for allowing payment performance with mail order method relating to wholesale sales and similar activities can be processed.

Söz konusu Kişisel Veriler, ödeme amacıyla sınırlı olarak işlenmelidir. Bu verilerin güvenliğini temin etmek için gereken önlemler alınmalı ve bu verilere erişim yalnızca yetkili personel ile sınırlandırılmalıdır. Bu verilerin işlem güvenliğini de temin etmek amacıyla yeniden ve başka bir şekilde kullanılmasını engelleyecek (güvenlik kodunun kullanım sonrası silinmesi ve benzeri) güvenliği temin edecek ileri düzey prosedürler uygulanmalıdır.

The said personal data should be processed as limited to payment purpose. Required measures should be adopted for procuring security of this data and access to this data should be limited to only authorized personnel. Advanced level procedures that shall prevent re-use and otherwise use for procuring transaction security of this data should be applied. (erasing security code after use and the like).

Şikâyet Verileri *Complaint Data*

Her Şirket için geçerli olmamakla beraber, 6502 sayılı Tüketicinin Korunması Hakkında Kanun uyarınca tüketici şikâyet ve taleplerinin yerine getirilmesine ilişkin olarak tüketicilerin ad, soyad, cinsiyet, e-mail, cep telefonu, ev telefonu, doğum tarihi, adres, beden, T.C. kimlik numarası ve benzeri Kişisel Veriler işlenebilir.

As not to be applicable for each Company, name, surname, gender, e-mail, mobile phone, home phone, date of birth, address, size, TR ID No, and similar personal data of consumers can be processed in relation to fulfilment of consumer complaints and requests as per the Consumer Protection Law no. 6502.

Söz konusu Kişisel Veriler, gelen şikâyet ve taleplerin gerekliliklerinin yerine getirilmesi, analiz yapılması ve benzeri amaçlar için işlenebilir.

The said personal data can be processed for fulfilling the requirements of incoming complaints and requests and performing analyses and similar purposes.

VI. ÖZEL NİTELİKLİ KİŞİSEL VERİLERİN İŞLENMESİ *VI. PROCESSING SPECIAL QUALITY PERSONAL DATA*

Şirket bünyesinde, Özel Nitelikli Kişisel Veriler, yalnızca kanuni ve idari / adli mercii gerekliliklerinin yerine getirilmesi ve Şirket'in işleyişi ile doğrudan ilgili olmak kaydıyla ve erişimi en üst düzeyde sınırlı ve güvenli olacak şekilde işlenebilir.

Special Quality Personal Data within the Company can be processed in a manner that their access shall be maximum limited and secure and provided that only requirements of legal and administrative/judicial authority be fulfilled and be directly associated with the functioning of the Company.

Söz konusu veriler, Kanun'a tam bir uyum göstermek kaydıyla,
Provided that the said data is in full compliance with the Law,

- (i) sağlık ve cinsel hayat dışındaki özel nitelikli kişisel veriler dışındaki veriler bakımından işlemenin kanunlarda açıkça öngörülmesi durumunda,
in cases where processing is expressly stipulated regarding the data other than special quality personal data and other than health and sexual life,

- (ii) sađlık ve cinsel hayata iliřkin veriler bakımından ise ancak, kamu sađlığının korunması, koruyucu hekimlik, tıbbî teřhis, tedavi ve bakım hizmetlerinin yürütülmesi, sađlık hizmetleri ile finansmanının planlanması ve yönetimi amacıyla, sır saklama yükümlülüđü altında bulunan kişiler veya yetkili kurum ve kuruluşlar tarafından işlenmesi durumunda

the data relating to health and sexual life is processed by the authorized institutions and organizations and the persons under the obligation of keeping secret for planning and managing the financing planning and healthcare services and executing protective medicine, medical diagnosis, treatment and care services and protecting public health,

Veri İlgilisi'nin rızası aranmaksızın işlenebilir. İstisnaların söz konusu olmadığı veya uygulanabilir olduklarına ilişkin şüphe duyulması halinde ise, açık rıza olmadan alınan Özel Nitelikli Kişisel Veriler derhal silinmeli, yok edilmeli veya anonim hale getirilmelidir.

They may be processed without seeking the consent of the Data Relevant Person. In cases where exceptions are not in question, or there is a doubt as to whether they are applicable, Special Quality Personal Data obtained without express consent should be immediately erased, destroyed or anonymized.

VII. KİŞİSEL VERİ İLGİLİSİNİ AYDINLATMA YÜKÜMLÜLÜĐÜ **VII. DISCLOSURE STATEMENT OF PERSONAL DATA RELEVANT PERSON**

Şirket, Kişisel Verilerin elde edilmesi sırasında, verisi işlenecek olan gerçek kişileri bilgilendirmekle yükümlüdür. Bu bilgilendirme yükümlülüđünün kapsamı, aşağıdaki gibidir:

The Company is liable for informing the real persons whose data is to be processed while acquiring the personal data. The scope of this disclosure obligation is as follows:

- Veri sorumlusunun ve varsa temsilcisinin kimliđi,
- Identification of data supervisor or its representative, if any,
- Kişisel Verilerin hangi amaçla işleneceđi,
- For what purpose the personal data is to be processed,
- İşlenen Kişisel Verilerin kimlere ve hangi amaçla aktarılabilceđi,
To whom and what purpose the processed personal data shall be transferred,

- Kişisel Veri toplamanın yönetimi ve hukuki sebebi ile,
Management and legal grounds of personal data collection,
- Veri İlgilisinin (III) başlığı altında belirtilen hakları.
Rights of the Data Relevant Person specified under the title of (III).

Şirket, bu konularda sistemlerinde işlemek üzere Üçüncü Kişilerden veri elde etme araçları vasıtasıyla gerekli bilgilendirmeleri yapmalı ve aydınlatma yükümlülüğünün gerçekleştirildiğinin ispatı için veri işlemeye ilişkin Veri Sahiplerinden aydınlatılmış onay almalıdır.

The Company should make required information via the means of acquiring data from Third parties so as to process the data in the systems in this regard and disclosed consent should be obtained from the Data Owners in relation to data processing for proving that disclosure statement has been fulfilled.

Kişisel Veriler, Şirket'in elektronik ticaret, perakende ve toptan satış dâhil tüm satış kanalları, şubeleri, internet siteleri, üçüncü kişilerden hizmet alınabilecek çağrı merkezi ve benzeri diğer tüm kanalları aracılığıyla otomatik ya da otomatik olmayan yollarla sözlü, yazılı veya elektronik olarak toplanabilecektir.

Personal data shall be able to collected either in writing or electronically with automatic or non-automatic means through all sales channels including electronic commerce, retail and wholesale, branches, Internet web sites, call centers to acquire service from third parties and all other similar channels.

- **Yazılı Şekilde Kişisel Veri Elde Edilmesi:**
- ***Acquiring Personal Data in Writing***

Yazılı şekilde, Kişisel Veri elde edilmesi sırasında Aydınlatma Yükümlülüğü yerine getirilecektir. Ayrıca, müşteri ilişkisi kurulan kişilerden alınacak İzinli İletişim Formları dâhil her tür form ve sözleşme, her ne kadar ilgili veri grubunun işlenmesi Kanun kapsamında istisna kapsamında değerlendirilebilse de, Kişisel Verilerin işlenmesine ilişkin Veri İlgilisinin açık rızasını gösterecek şekilde revize edilmelidir. Müşteri ilişkilerinde, Kanun'a uyumu tevsik eder nitelikteki yeni formlar, belgeler ve bilgilendirmeler kullanılmalı; tüm ilgili çalışanlar bu konuda gerçek kişiye yeterli düzeyde detaylı bilgiyi sağlamak ve referansları göstermek konusunda eğitilmelidir. Mutlak surette, Kişisel Verilerin aydınlatılmış onaylarının yer aldığı yazılı formlar ile elde edilmesi temin edilmelidir.

The disclosure statement shall be fulfilled during acquiring Personal data in writing. Also, even if all kinds of forms and contracts including Consented

Communication Forms to be obtained from the persons with whom customer relationship has been established are considered within the scope of the exception under the Law as regards processing the relevant data group, it should be revised in a manner that it shall show express consent of the Data Relevant Person in regard to processing personal data. New forms, documents and information evidencing their compliance with the Law in customer relationships should be used; all relevant employees should be trained in the issue of providing detailed information in sufficient level to a real person in this regard and showing references. Personal data should be procured to be acquired with the written forms containing disclosure consents at all times.

- **Sözlü Şekilde Kişisel Veri Elde Edilmesi:**
- **Acquiring Personal Data Verbally:**

Çağrı Merkezi v.b. aracılığıyla veri elde edilmesi sırasında Kişisel Verilerin işlenmesine ilişkin aydınlatma yükümlülüğüne ilişkin bilgi verilmelidir. Sözlü veri elde edilmesi sırasında, önceden bilgi verilmek kaydıyla görüşmenin kaydedildiği hatırlatılmalı ve Kişisel Verilerinin Aydınlatma Metni kapsamında işleneceği konusunda onay verildiği teyit edilmelidir. Çalışan ve Çağrı Merkezi, iş yapış süreçleri bu çerçevede yeniden gözden geçirilmeli ve uygulamaya konulmalıdır.

The information relating to disclosure statement obligation should be provided in regard to processing personal data while acquiring data through Call Center etc. It should be reminded that negotiation is recorded provided that prior consent is granted during acquiring verbal data and it should be verified that the consent has been granted in the issue indicating that it is processed within the scope of the Disclosure Text of Personal Data. Throughput processes of Employee and Call Center should be reviewed and implemented within this framework.

- **Elektronik Ortamda Kişisel Veri Elde Edilmesi:**
- **Acquiring Personal Data in Electronic Environment:**

Elektronik ticaret kanalları ve/veya Şirket'in diğer internet kanalları ile elde edilen veriler de dâhil olmak üzere, Kişisel Verilerin elde edilmesi ve işlenmesini gerektiren mesafeli satış sözleşmeleri dâhil tüm sözleşme ve belgeler / bağlantı adresleri / internet sayfaları Kişisel Verilerin işlenmesine ilişkin aydınlatma yükümlülüğünü yerine getirecek şekilde revize edilmelidir. Aydınlatma Metni internet sayfalarından ulaşılabilecek şekilde, Şirket'in internet sitesinde yer almalı ve veri elde edilmesini gerektirebilecek her bağlantı adresinde veri elde edilmesi için Şirket tarafından veri işlenmesinin onaylanmasını gerektiren sistemler kurulmalıdır. Mümkün olduğu kadar Kişisel Verilerin işlenmesine onay verildiği açıkça işaretlenmedikçe, girilen hiçbir bilgi

ve belge otomatik olarak Şirket sistemine kaydedilmemeli ve/veya işlenmemelidir.

All contracts and documents/connection addresses / Internet web sites including distant sales contracts requiring acquiring and processing Personal data including the data acquired with electronic commerce channels and/or other Internet channels of the company should be revised in a manner that they shall fulfil disclosure statement obligation regarding the processing personal data. Disclosure Text should be included on the Internet web site of the Company in a manner that shall be accessed from the pages of Internet web site and the systems requiring approval of data processing by the Company should be used for acquiring data at each connection address that shall require that the Company is included on the Internet web site or data is acquired in a fashion that can be accessed from Internet web pages. To the extent consent has been granted to the processing of Personal Data as far as possible is not clearly marked, no information and document so entered should not be recorded and/or processed to the Company system as the entered information and document.

VIII. ŞİKÂYET SÜREÇLERİNE İLİŞKİN PROSEDÜRLER **VIII. PROCEDURES RELATING TO COMPLAINT PROCESSES**

Kişisel Verileri Şirket tarafından işlenen Veri Sahipleri tarafından yapılacak şikâyetler, Şirket tarafından en kısa süre içerisinde ve en geç 30 gün içerisinde cevaplandırılmalı ve sonuçlandırılmalıdır.

The complaint to be made by the Data Owner whose Personal Data Company is defined by the Data Owners as far as possible and it should be responded within maximum 30 days and should be concluded.

Veri Sahibi, talep ve şikâyetlerini Şirket'e ilgili birim tarafından kimlik kontrolü yapılmak kaydıyla şahsen veya noter onaylı vekâlet sunulması kaydıyla vekâleten yapabilirler. Noter kanalı ile yapılan başvurular ve güvenli elektronik imza kullanılmak kaydıyla kayıtlı elektronik posta adresleri ile Şirketin e-posta adresine yapılabilir.

Data Owner can perform its request and complaint in proxy provided that personal or notarized power of attorney are included in person without prejudice to identification inspection by the relevant unit to the Company. Application made with notary channel can be made to the e-mail address of the Company with registered e-mails provided that secure electronic signature is to be used.

E-posta ve telefon yoluyla gelen taleplerle ilgilenen Şirket çalışanlarının Şirket tarafından tutulan herhangi bir kişisel bilginin açıklanması konusunda dikkatli olmaları konusunda eğitimden geçirilmelidirler. Bu çalışanlar, özellikle;

- Kişisel Verinin, kişisel veriyi almaya yönelik bir hakka sahip olan/yetkisi olan kişiye verildiğinden emin olmak için, çağrı yolu ile ulaşan kişinin kimliğini kontrol etmelidirler;
- Çalışanlar, arayanın kimliğinden emin olmadıkları ya da kimliklerinin kontrol edilemediği bir çağrı alırlarsa, arayanın talebini yazılı olarak iletmesini önermelidirler.
- Zor durumlarda yardım için müdürlerine başvurmalıdırlar. Hiç kimse Kişisel Verinin açıklanması için zorlanmamalıdır.

The Company should be subject to training and they should be very careful on the issue of disclosure of personal information kept by the Company as regards those dealing with the request via e-mail and phone. These employees should especially;

- *The identity of the person accessing via call should be inspected for ensuring that the personal data is provided to the person entitled/authorized to receive personal data.*
- *If the employees are not sure of the caller identity or fail to inspect their identities and receive a call under these circumstances, it should be recommended that the caller request should be communicated in writing.*
- *Managers should be consulted for help in difficult conditions. No one should be forced to disclosure of personal data.*

Bir çalışanın, yukarıdaki prosedürlere tabi olmak kaydıyla, Veri Sahiplerinden bir bildirim / talep alması halinde, bu durum bu bildirim / talebin alınmasını takiben derhal Şirketin ilgili birimine yazılı şekilde rapor edilmeli ve bu taleplere cevap verilirken, söz konusu birimin tüm talimatlarına uygun hareket edilmelidir. Söz konusu iş birimi, şikâyetleri / talepleri çözümlmek için ilgili iş biriminden ve destek birimlerinden bu konuda yetkilendirilmiş kişilerle bağlantı kurmalıdır.

Provided that an employee receives a notification/request from the Data Owner provided that an employee is subject to the procedures above, this case should be immediately reported in writing to the relevant department of the Company with immediate effect following obtaining this notification/request and it should be acted in compliance with all instructions of the said unit while responding to these requests. The said business unit should establish a connection with the persons authorized in this regard from the relevant business unit and support units for solving these complaints/requests.

Veri Sahibinden gelen talepler özenli bir şekilde rapor edilmeli ve gözden geçirilmeli, Şirket tarafından yetkilendirilmiş kişiler, talebin niteliğini de göz önünde bulundurarak, en fazla 30 gün içerisinde olmak şartıyla, mümkün olan en kısa sürede ve Veri Sahibine ek bir masraf yansıtılmaksızın söz konusu şikâyetler yanıtlanacak ve talepler uygulanabilir olması halinde yerine getirilmelidir.

The requests from Data Owner should be meticulously reported and reviewed; the persons authorized by the Company should consider the nature of the request and the said complaints and requests should be fulfilled to the extent they are applicable without incurring an additional expense to the Data Owner and within the shortest time possible provided that it shall be within maximum 30 days.

Kişisel Verilerin silinmesi, yok edilmesi ve anonim hale getirilmesi de dâhil, her tür Veri Sahibi talebinin incelenmesine ilişkin takip eden süreç aşağıdaki şekilde olmalıdır:

The following process in relation to review of the request of the Data Owner including erasing, destruction and anonymization of the personal data should be as follows:

- Şirketin Kişisel Verilerin Korunması ile ilgili yetkilendirmiş olduğu kişiler (komite/birim), talebin/şikayetin geçerli olup olmadığına ve kimlik teyidi ya da ek bilginin gerekli olup olmadığına karar vermek için talebin ilk değerlendirmesini yapmalıdırlar.

- *First evaluation of the request should be made for deciding whether or not identification verification or additional information is required and the request/complaint is applicable or not by the relevant authorized persons (committee/unit) in regard to Personal data protection of the company.*

- İlgili birim, birey ile yazılı olarak bağlantı kurarak, Veri Sahibinin erişim talebinin alındığını teyit etmeli, gerektiği takdirde kimlik teyidi, ek bilgi talebi ya da başvurunun yeterli görülmemesi olması durumunda talebi reddedilecektir.

-*The relevant unit should verify the receipt of the access request of the Data Owner by establishing a connection in writing with the individual; if required, its request shall be rejected if identification confirmation, additional information or application's being insufficient.*

- Tüm ilgili elektronik ve basılı dosyalama sistemleri üzerinde bir arama düzenlenmelidir.

- *A search should be arranged on all relevant electronic and printed filing systems.*

- İlgili birim, komplike durumları, özellikle de talebin üçüncü kişiler ile ilgili bilgiyi içerdiği ya da Kişisel Verilerin ifşa edilmesinin ticari gizliliğe ya da hukuki süreçlere zarar verebileceği durumları, şirket içi ilgili birimler ya da üçüncü kişi danışmanlara sevk edebilir ve talebin yanıtlanması konusunda destek alabilir.

-The Relevant unit may submit the complicated statuses, especially in cases where the information related to the persons or disclosure of Personal data can submit to in-house relevant units or third-party consultant and may get support in the issue of responding the request.

- İlgili birim, talep edilen bilgileri kolaylıkla okunabilir bir formatta düzenlemelidir.

- It should issue in a readable format with ease in a format as regards the requested information.

İlgili birim, Şirket adına Veri Sahibinin talebini kabul edebilir ya da gerekçesini açıklayarak yazılı ya da elektronik ortamda reddedebilir. Bununla sınırlı olmaksızın, özellikle Kanun'un uygulanmasına ilişkin istisnalardan birinin söz konusu olduğu hallerde talep reddedilebilecektir. Veri Sahibinin talebi kabul edilirse, talep Şirket'in ilgili birimleri tarafından derhal yerine getirilecektir.

The relevant unit may accept the request for Data Owner on behalf of the Company or describe its justification and reject the same in writing or electronically. Without limitation to the foregoing, in case of exceptions relating to enforcement of the Law, the request can be able to be rejected. If the request of the Data Owner is accepted, the request shall be immediately fulfilled by the relevant unit of the Company.

Şikâyet sahibi, Şirket tarafından verilecek cevap ya da tespite tamamen ya da kısmen itiraz edebilecek ve ilgili birim veya Şirket çalışanını bu konuda bilgilendirebilecektir. İlgili çalışan derhal ilgili birime bilgi verecektir. Böyle bir durumda, şikâyet talebi yeniden değerlendirilecek ve nihai olarak cevaplandırılacaktır.

The complaint owner shall be able to wholly or partially object to the response or determination to be given by the Company and the relevant unit or the Company employee shall be able to be informed about this issue. – The relevant employee shall provide the relevant unit with the information. In such a case, the request for complaint shall be re-considered and shall be finally responded.

Uygulanacak prosedür ve sürelerle ilişkin ilk sürelerle uygulanabilir prosedür ve süreler geçerli olacak olup bu durum Kanun'un öngördüğü sürelerin kesilmesi veya durdurulması anlamına gelmeyecektir. Zira, ikinci kez değerlendirmeye ilişkin talepler kanuni bir yükümlülük kapsamında değil salt müşteri memnuniyeti açısından yeniden değerlendirilecektir.

The procedures and periods to be applied to the initial periods in regard to applicable procedures and periods shall be valid and this case should not be construed that this case interrupts or stop the period stipulated in the Law. Indeed, the requests relating

to the second time evaluation are not within the scope of a legal obligation and shall be re-considered regarding only customer satisfaction.

Kanun uyarınca, Veri Sahibinin ilk şikâyet başvurusuna verilecek ilk yanıttan itibaren, Şirket'in cevabını öğrendiği tarihten itibaren otuz ve her hâlde ilk başvuru tarihinden itibaren altmış gün içinde Kurula başvurma hakkı vardır ve söz konusu sürelere riayet edilmesi hak düşürücü niteliktedir.

As per the Law, the Data Owner is entitled to apply for the Board within sixty days as of the first application date at all times and thirty as of the date when the response of the Company is learned and adhering to the said periods is in foreclosure of his response of the Company as of the first response where the first complaint application is to be provided.

IX. KİŞİSEL VERİLERİN KORUNMASI KURUMU İLE İLETİŞİM IX. PROTECTING PERSONAL DATA CORPORATION AND COMMUNICATION

Şirket, devlet sırlarını içeren bilgi ve belgeler hariç olmak üzere; Kurulun, inceleme konusuyla ilgili istemiş olduğu bilgi ve belgeleri 15 gün içinde göndermek ve gerektiğinde yerinde inceleme yapılmasına imkân sağlamak zorundadır.

Excluding the information and documents containing the state secrets, the Company is obligated to submit the information and documents requested by the Board in relation to its field within 15 days and to allow an investigation to be conducted in place when it is necessary.

Şirket'in ilgili birimi Kurum ile yapılacak yazışmaları gerçekleştirecek iş birimi olarak belirlenmeli ve çalışanlar, Kişisel Verinin korunmasına ilişkin Kurul ile her türlü iletişimi ilgili birime yönlendirmelidirler.

The relevant unit of the Company should be determined as the business unit that shall perform the correspondences to be made with the Board and they should direct all kinds of communications to the relevant unit with the Board in relation to the protection of personal data.

Şirket çalışanlarının, Kurul'un re'sen ya da şikâyet üzerine yapılan soruşturmanın sonucunda verilen kararlarına, gecikmesiz ve bildirimden itibaren en geç 30 gün içerisinde uyulması sağlanmalıdır.

It should be ensured that the decisions rendered as a result of the investigation conducted upon the complaint or ex officio by the Board should be adhered to without delay and within 30 days at the latest as of the notification.

Şirket, Kurulun aktif olarak faaliyete geçmesi ve Kişisel Verileri Koruma Kurumu nezdinde oluşturulacak başkanlık teşkilatının oluşumunu takiben Kurulun gözetiminde ve Kişisel Verileri Koruma Kurumu Başkanlığı tarafından kamuya açık olarak tutulacak Veri Sorumluları Sicili'ne, Kurul tarafından Veri Sorumluları Siciline kayıt zorunluluğuna getirilecek istisnalara tabi olmadıkça, kayıt olmalıdır.

The Company should be registered to the Data Relevant Person Registration to be kept publicly by the Department of Personal Data Protection Institution and under the supervision of the Board following establishment of presidency organization by being formed within the Personal Data Protection Institution and after the Board actively operates unless they are subject to the exceptions to be brought forth to the registration obligation of the Data Relevant Persons.

X. KİŞİSEL VERİLERİN KORUNMASI VE İŞLENMESİ POLİTİKASI YÖNETİM YAPISI

X. PERSONAL DATA PROTECTION AND PROCESSING POLICY MANAGEMENT STRUCTURE

Şirket tarafından KVK Kanunu düzenlemelerine uygun hareket edilmesi ve Kişisel Verilerin Korunması ve İşlenmesi politikası ve prosedürlerini yürütmek üzere Karar Kurulu ve birim/komite oluşturmalıdır.

A Decision Board and unit/committee should be formed by the company for executing the policy and procedures on Personal Data Protection and Processing Policy and acting in compliance with the regulations of Personal Data Protection and Processing Policy.

Bu Karar Kurulu ve birim/komitenin görevleri;
Duties of this Decision Board and unit/committee;

1- Kişisel Verilerin Korunması ve İşlenmesi ile ilgili kararlar alarak, üst yönetime sunulmak üzere üst kurula iletmek,

Adopting decisions relating to Personal Data Protection Policy and communicating them to be submitted to the top management,

2- Kişisel Verilerin Korunması ve İşlenmesi ile ilgili Politika'da değişiklikler yapmak, Politikanın uygulanmasını ve denetimini sağlamak,

Making amendments in Personal Data Protection and Processing Policy and ensuring implementation and audit of the Policy,

3- KVK Kanunu ve ilgili mevzuat çerçevesinde yapılması gereken hususları tespit etmek,

Determining the considerations to be performed within the framework of Personal Data Protection Law and the relevant legislation,

- 3- Kişisel Veri sahiplerinin başvurularını değerlendirmek,
Evaluating the applications of personal data owners,
- 4- Kişisel Verilerin Korunması ile ilgili gelişmeleri takip etmek, ilgilileri bilgilendirmek suretiyle uygulanmasını sağlamak ve gerekli önlemleri almak,
Following up the developments relating to Personal Data Protection and informing those concerned and ensuring their implementation and taking required measures

XI. POLİTİKA’NIN UYGULANMASINA İLİŞKİN İSTİSNALAR **XI. EXCEPTIONS RELATING TO IMPLEMENTATION OF THE POLICY**

KVKK. 28. Maddesi uyarınca öngörüldüğü üzere, Kanun’un uygulanmayacağı aşağıdaki hallerde, işbu Politika da uygulanmayacaktır:

As stipulated under Article 28 of Personal Data Protection Law, this Policy shall not also be implemented in the following cases where the Law is not implemented:

— Kişisel Verilerin, üçüncü kişilere verilmemek ve veri güvenliğine ilişkin yükümlülüklerle uyulmak kaydıyla gerçek kişiler tarafından tamamen kendisiyle veya aynı konutta yaşayan aile fertleriyle ilgili faaliyetler kapsamında işlenmesi;

- *Provided that Personal data is not provided to the third parties and the obligations relating to data security are adhered to, processing the same within the scope of the operations related to the family individuals living with fully itself or living in the same housing by the real persons;*

— Kişisel Verilerin resmi istatistik ile anonim hâle getirilmek suretiyle araştırma, planlama ve istatistik gibi amaçlarla işlenmesi;

- *Processing the purposes of investigation, planning and statistics by anonymizing the personal data with official statistics;*

— Kişisel Verilerin millî savunmayı, millî güvenliği, kamu güvenliğini, kamu düzenini, ekonomik güvenliği, özel hayatın gizliliğini veya kişilik haklarını ihlal etmemek ya da suç teşkil etmemek kaydıyla, sanat, tarih, edebiyat veya bilimsel amaçlarla ya da ifade özgürlüğü kapsamında işlenmesi;

- *Provided that the personal data does not breach the natural defence, national security, public security, public order, economic security and confidentiality of private life or personality rights are not breached and does not constitute a crime, processing the same within the framework of artistic, historic, literature or scientific purposes or freedom of speech;*

— *Kişisel Verilerin millî savunmayı, millî güvenliği, kamu güvenliğini, kamu düzenini veya ekonomik güvenliği sağlamaya yönelik olarak kanunla görev ve yetki verilmiş kamu kurum ve kuruluşları tarafından yürütülen önleyici, koruyucu ve istihbari faaliyetler kapsamında işlenmesi;*

- *Processing the personal data within the scope of preventive, protective and intelligence operations executed by public institutions and organizations so authorized and office with the law in regard to ensuring national defence, national security, public safety, public order or economic security;*

— *Kişisel Verilerin soruşturma, kovuşturma, yargılama veya infaz işlemlerine ilişkin olarak yargı makamları veya infaz mercileri tarafından işlenmesi.*

— *Processing the personal data by judicial or enforcement authorities in relation to the investigation, proceedings, litigation or execution procedures.*

Aydınlatma yükümlülüğü hariç olmak üzere, Veri Sahipleri aşağıdaki istisnaların birinin varlığı halinde Kanun ve işbu Politika'da düzenlenen haklarını kullanamayacaktır:

Excluding disclosure statement, the Data Owners shall not be able to exercise the rights set out in this Policy and the Law in case of presence of the following exceptions:

— *Kişisel Veri işleminin suç işlenmesinin önlenmesi veya suç soruşturması için gerekli olması;*

- *Processing personal data being required for prevention of committing an illegal act or offence investigation;*

— *Veri Sahibinin kendisi tarafından alenileştirilmiş Kişisel Verilerin işlenmesi;*

- *Processing personal data made public approach armature the Data Owner itself;*

— Kişisel Veri işleminin kanunun verdiği yetkiye dayanılarak görevli ve yetkili kamu kurum ve kuruluşları ile kamu kurumu niteliğindeki meslek kuruluşlarınca, denetleme veya düzenleme görevlerinin yürütülmesi ile disiplin soruşturma veya kovuşturması için gerekli olması;

- *Processing personal data being required for disciplinary investigation or prosecution and executing audit or regulatory duties by assigned and authorized public institutions and organizations and professional organizations in nature of public institutions by the power granted by the law*

- Kişisel Veri işleminin bütçe, vergi ve mali konulara ilişkin olarak Devletin ekonomik ve mali çıkarlarının korunması için gerekli olması.

- *Processing personal data being required for protecting the economic and financial interest of the State in relation to the budget, tax and financial matters.*

Yukarıda sayılanlar dışında, tamamen veya kısmen otomatik olan ya da herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla elde edilen Kişisel Veriler de bu Politika'nın kapsamı dışındadır. Bu çerçevede, Şirket nezdinde herhangi bir veri kayıt sisteminde yer almayan tüm veriler bakımından Kanun ve işbu Politika uygulanmayacaktır. Şirket'in söz konusu veriler ile ilgili sorumluluğu T.C. Anayasası ve Türk Ceza Kanunu hükümleri ile sınırlı olacaktır.

Except for the foregoing, the personal data that is wholly or partially automatic or acquired by non-automatic means provided that it shall be a part of any data registration system are outside the scope of this Policy. In this context, the Law and this Policy shall not be applied in terms of all data not contained in any data registration system within the Company. The responsibility of the Company in relation to the said data shall be limited to the provisions of Constitution of the Republic of Turkey and Turkish Penal Code.

XII. İYİLEŞTİRME VE DEĞİŞİKLİKLER **XII. IMPROVEMENTS AND AMENDMENTS**

Şirket çalışanlarının Kişisel Veriler konusu ve Kanun hakkında soruları ya da sorunlarını görevlendirecek birime yöneltmesi uygun olur.

It would be appropriate for the Company employees should direct their questions or issues regarding the field of Personal data and the Law to the unit to be assigned.

Kanun uyarınca hazırlanacak ve yürürlüğe girecek Yönetmelik ve diğer ikincil mevzuat uyarınca gerekli değişiklikler yapılarak güncelleştirilmesi gerekecektir.

Required amendments shall be made and updated as per the Regulation and other secondary legislation to be prepared and to be effective as per the Law.

SONUÇ VE SORUMLULUK **CONCLUSION AND RESPONSIBILITY**

Şirket, 6698 Sayılı Kişisel Verilerin Korunması Kanunu gereğince Türkiye Cumhuriyeti Anayasası ve Türk Ceza Kanunu hükümleri ile kişisel veri korumasına ilişkin uluslararası genel ilkelere uyumlu tüm süreçleri yönetmeli ve yerine getirmelidir.

The Company should manage and fulfil all processes in compliance with general international principles in relation to personal data protection and the provisions of the Constitution of the Republic of Turkey and Turkish Penal Code as per the Personal Data Protection Law no. 6698.

Bu İşlemler yerine getirilirken Kişisel Verilerin Koruma Kurulu tarafından 31.01.2018 tarih ve 2018/10 sayılı kararı göz önünde bulundurulmalıdır.

The decision dated 31/01/2018 and no. 2018/10 of the Personal Data Protection Board should be taken into consideration while fulfilling these procedures.

Özel Nitelikli Kişisel Verilerin İşlenmesinde Veri Sorumlularınca Alınması Gereken Yeterli Önlemler

6698 sayılı Kişisel Verilerin Korunması Kanununun (Kanun) 6 ncı maddesinin (4) numaralı fıkrasında, “Özel nitelikli kişisel verilerin işlenmesinde, ayrıca Kurul tarafından belirlenen yeterli önlemlerin alınması şarttır.” hükmü yer almaktadır.

Bu çerçevede, Kanunun 22 nci maddesinin (1) numaralı fıkrasının (ç) ve (e) bentleri uyarınca özel nitelikli kişisel veri işleyen veri sorumluları tarafından alınması gereken yeterli önlemler Kişisel Verileri Koruma Kurulu tarafından aşağıdaki şekilde belirlenmiştir:

- 1- Özel nitelikli kişisel verilerin güvenliğine yönelik sistemli, kuralları net bir şekilde belli, yönetilebilir ve sürdürülebilir ayrı bir politika ve prosedürün belirlenmesi,
- 2- Özel nitelikli kişisel verilerin işlenmesi süreçlerinde yer alan çalışanlara yönelik,
 - a) Kanun ve buna bağlı yönetmelikler ile özel nitelikli kişisel veri güvenliği konularında düzenli olarak eğitimler verilmesi,
 - b) Gizlilik sözleşmelerinin yapılması,
 - c) Verilere erişim yetkisine sahip kullanıcıların, yetki kapsamlarının ve sürelerinin net olarak tanımlanması,
 - ç) Periyodik olarak yetki kontrollerinin gerçekleştirilmesi,
 - d) Görev değişikliği olan ya da işten ayrılan çalışanların bu alandaki yetkilerinin derhal kaldırılması. Bu kapsamda, veri sorumlusu tarafından kendisine tahsis edilen envanterin iade alınması,
- 3- Özel nitelikli kişisel verilerin işlendiği, muhafaza edildiği ve/veya erişildiği ortamlar, elektronik ortam ise
 - a) Verilerin kriptografik yöntemler kullanılarak muhafaza edilmesi,
 - b) Kriptografik anahtarların güvenli ve farklı ortamlarda tutulması,
 - c) Veriler üzerinde gerçekleştirilen tüm hareketlerin işlem kayıtlarının güvenli olarak loglanması,
 - ç) Verilerin bulunduğu ortamlara ait güvenlik güncellemelerinin sürekli takip edilmesi, gerekli güvenlik testlerinin düzenli olarak yapılması/yaptırılması, test sonuçlarının kayıt altına alınması,
 - d) Verilere bir yazılım aracılığı ile erişiliyorsa bu yazılıma ait kullanıcı yetkilendirmelerinin yapılması, bu yazılımların güvenlik testlerinin düzenli olarak yapılması/yaptırılması, test sonuçlarının kayıt altına alınması,
 - e) Verilere uzaktan erişim gerekiyorsa en az iki kademeli kimlik doğrulama sisteminin sağlanması,

- 4- Özel nitelikli kişisel verilerin işlendiği, muhafaza edildiği ve/veya erişildiği ortamlar, fiziksel ortam ise
- Özel nitelikli kişisel verilerin bulunduğu ortamın niteliğine göre yeterli güvenlik önlemlerinin (elektrik kaçağı, yangın, su baskını, hırsızlık vb. durumlara karşı) alındığından emin olunması,
 - Bu ortamların fiziksel güvenliğinin sağlanarak yetkisiz giriş çıkışların engellenmesi,
- 5- Özel nitelikli kişisel veriler aktarılabaksa
- Verilerin e-posta yoluyla aktarılması gerekiyorsa şifreli olarak kurumsal e-posta adresiyle veya Kayıtlı Elektronik Posta (KEP) hesabı kullanılarak aktarılması,
 - Taşınabilir Bellek, CD, DVD gibi ortamlar yoluyla aktarılması gerekiyorsa kriptografik yöntemlerle şifrelenmesi ve kriptografik anahtarın farklı ortamda tutulması,
 - Farklı fiziksel ortamlardaki sunucular arasında aktarma gerçekleştiriliyorsa, sunucular arasında VPN kurularak veya sFTP yöntemiyle veri aktarımının gerçekleştirilmesi,
 - Verilerin kağıt ortamı yoluyla aktarımı gerekiyorsa evrakın çalınması, kaybolması ya da yetkisiz kişiler tarafından görülmesi gibi risklere karşı gerekli önlemlerin alınması ve evrakın "gizlilik dereceli belgeler" formatında gönderilmesi
- gerekir.
- 6- Yukarıda belirtilen önlemlerin yanı sıra Kişisel Verileri Koruma Kurumunun internet sitesinde yayımlanan Kişisel Veri Güvenliği Rehberinde belirtilen uygun güvenlik düzeyini temin etmeye yönelik teknik ve idari tedbirler de dikkate alınmalıdır.



Sufficient Measures Required to be Taken by Data Supervisors in Processing Special Quality Personal Data

The paragraph (4) of Article 6 of the Personal Data Protection Law (Law) no. 6698 sets forth that "Sufficient measures designated by the Board should also be taken in processing Special Quality Personal Data."

Within this framework, as per (d) and (f) clauses of the paragraph no. 1 of Article 22 of the Law, sufficient measures required to be taken by data supervisors processing Special Quality Personal Data are determined as follows by Personal Data Protection Board:

- 1- Determination of a systematic, sustainable and manageable separate policy and procedure with clear rules intended for the security of Special Quality Personal Data,*
- 2- For employees in the processes of processing Special Quality Personal Data,*
 - a) Providing regular training on the issue of Special Quality Personal Data with the Law and its affiliated regulation,*
 - b) Executing confidentiality contracts*
 - c) Clearly defining the users holding access authority to the data and authority scope and periods,*
 - d) Performing periodic authority checks,*
 - e) Immediately removing the authorities of those subject to post change or dismissal in this field. In this context, accepting the return of inventories allocated to itself by data supervisor,*
- 3- If the environments where Special Quality Personal Data is processed, maintained and/or accessed are an electronic environment*
 - a) Maintaining data by using cryptographic methods,*
 - b) Keeping cryptographic keys safe and different environments,*
 - c) Transaction records of all activities performed on data should be logged securely,*
 - d) Continuously following up security updates pertaining to the environment of data, performing/causing to perform regularly required security tests, recording test results,*
 - e) If data is accessed via software, user authorization pertaining to this software should be made and security tests of this software should be regularly performed or caused to be performed, recording test results,*
 - f) If access is required remotely to data, providing minimum two-level authentication system,*



- 4- *If the environments where Special Quality Personal Data is processed, maintained and/or accessed are a physical environment*
 - a) *Ensuring that sufficient safety measures are taken as to environment nature where Special Quality Personal Data is available (electrical leakage, fire, flood, theft, etc.)*
 - b) *Preventing unauthorized entrance and exit by ensuring the physical security of these environments,*

- 5- *If Special Quality Personal Data is to be transferred*
 - a) *If data is required to be transferred via e-mail, transferring the same with corporate e-mail address having a password or using Registered Electronic Mail (KEP) account,*
 - b) *If it is required to be transferred via environments such as CD, DVD and portable memory, they should be encoded with cryptographic methods and keeping cryptographic keys in different environments,*
 - c) *If the transfer is carried out among the servers in different physical environments, VPN is installed among the server or performing data exchange with sFTP method,*
 - d) *If data is required to be transferred via the paper environment, taking required measures against the risk such as theft of document, loss of it or accessing it by unauthorized persons and the document should be sent in "confidentiality degree documents".*

- 6- *Besides the measures above, technical and administrative measures should be taken into consideration in regard to providing appropriate security level specified in Personal Data Security Guide published in the Internet web site of Personal Data Protection Institution.*

