

PAGETEL Ltd. Şti.
İzmir- TÜRKİYE

KİŞİSEL VERİLERİN KORUNMASI VE İŞLENMESİ, KİŞİSEL VERİ SAKLAMA VE İMHA POLİTİKASI

Protection, Processing Storage and Destruction of Personal Data Policy
Kod/Code # FR-03.40

Tarih / Date :

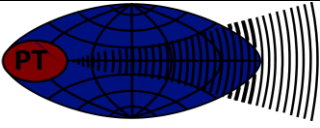
Sayfa / Page : 1 / 54

İÇİNDEKİLER

TABLE OF CONTENTS

İÇİNDEKİLER.....	1
KISALTMALAR VE KAVRAMLAR	1
1. GİRİŞ	3
2. KİŞİSEL VERİLERİN KORUNMASINA İLİŞKİN HUSUSLAR ..4	
3. KİŞİSEL VERİLERİN İŞLENMESİNE İLİŞKİN HUSUSLAR8	
4. ŞİRKETİMİZ TARAFINDAN İŞLENEN KİŞİSEL VERİLERİN KATEGORİZASYONU, İŞLENME AMAÇLARI VE SAKLANMA SÜRELERİ	13
5. ŞİRKET TARAFINDAN İŞLENEN KİŞİSEL VERİLERİN SAHİPLERİNE İLİŞKİN KATEGORİZASYON.....	30
6. ŞİRKET TARAFINDAN KİŞİSEL VERİLERİN AKTARILDIĞI ÜÇÜNCÜ KİŞİLER VE AKTARILMA AMAÇLARI	37
7. KİŞİSEL VERİLERİN KANUNDAKİ İŞLEME ŞARTLARINA DAYALI VE BU ŞARTLARLA SINIRLI OLARAK İŞLENMESİ ..39	
8. KİŞİSEL VERİLERİN SİLİNMESİ, YOK EDİLMESİ VE ANONİMLEŞTİRİLMESİ ŞARTLARI.....	43
9. KİŞİSEL VERİ SAHİPLERİNİN HAKLARI; BU HAKLARIN KULLANILMASI VE DEĞERLENDİRİLMESİ METODOLOJİSİ 45	
10. ŞİRKET KİŞİSEL VERİLERİN KORUNMASI VE İŞLENMESİ POLİTİKASI'NIN DİĞER POLİTİKALARLA OLAN İLİŞKİSİ	48

TABLE OF CONTENTS.....	1
ABBREVIATIONS AND CONCEPTS.....	1
1. INTRODUCTION	3
2. ISSUES CONCERNING THE PROTECTION OF PERSONAL DATA.....	4
3. ISSUES CONCERNING THE PROCESSING OF PERSONAL DATA.....	8
4. CATEGORISATION, PROCESSING PURPOSES AND STORAGE PERIODS OF PERSONAL DATA PROCESSED BY THE COMPANY	13
5. CATEGORISATION RELATED TO THE OWNERS OF PERSONAL DATE PROCESSED BY THE COMPANY.....	30
6. THIRD PARTIES WHO ARE TRANSFERRED PERSONAL DATA BY THE COMPANY AND PURPOSES OF TRANSFER.37	
7. PROCESSING OF PERSONAL DATA BASING ON AND LIMITED TO THE PROCESSING CONDITIONS IN THE ACT ..39	
8. CONDITIONS FOR THE DELETION, DESTRUCTION AND ANONYMIZATION OF PERSONAL DATA	43
9. RIGHTS OF THE OWNERS OF PERSONAL DATA; METHODOLOGY FOR THE EXERCISE AND EVALUATION OF SUCH RIGHTS.....	45
10. RELATIONSHIP OF THE COMPANY'S POLICY FOR THE PROTECTION AND PROCESSING OF PERSONAL DATA WITH OTHER POLICIES	48



PAGETEL Ltd. Şti.
İzmir- TÜRKİYE

KİŞİSEL VERİLERİN KORUNMASI VE İŞLENMESİ, KİŞİSEL VERİ SAKLAMA VE İMHA POLİTİKASI

Protection, Processing Storage and Destruction of Personal Data Policy
Kod/Code # FR-03.40

Tarih / Date :

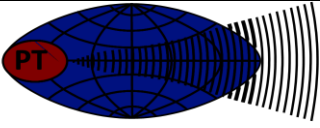
Sayfa / Page : 2 / 54

KISALTMALAR VE KAVRAMLAR

KVKK Kanunu	7 Nisan 2016 tarihli ve 29677 sayılı Resmi Gazete'de yayımlanan 6698 sayılı Kişisel Verilerin Korunması Kanunu
GDPR	EU (Avrupa Birliği) General Data Protection Regulation
Anayasa	9 Kasım 1982 tarihli ve 17863 sayılı Resmi Gazete'de yayımlanan 7 Kasım 1982 tarihli ve 2709 sayılı Türkiye Cumhuriyeti Anayasası
Veri İşleyen	Verilerin teknik olarak depolanması, korunması ve yedeklenmesinden sorumlu olan kişi ya da birim hariç olmak üzere veri sorumlusu organizasyonu dışında ve veri sorumlusundan aldığı yetki ve talimat doğrultusunda kişisel verileri işleyen kişi.
Veri Sahibi/İlgili	ŞİRKET ve/veya ŞİRKET'in bağlı şirketleri/iştiraklerinin ticari ilişki Kişi/İlgili Kişiler içinde bulunduğu çalışanları, müşterileri, iş ortakları, hissedarları, yetkilileri, potansiyel müşterileri, aday çalışanları, stajyerleri, ziyaretçileri, tedarikçileri, iş birliği içinde çalıştığı kurumların çalışanları, üçüncü kişiler ve burada sayılanlarla sınırlı olmamak üzere diğer kişiler gibi kişisel verisi işlenen gerçek kişi.
Veri Sorumlusu	Kişisel verilerin işleme amaçlarını ve vasıtalarını belirleyen, veri kayıt sisteminin kurulmasından ve yönetilmesinden sorumlu olan gerçek veya tüzel kişi.
Açık Rıza	Belirli bir konuya ilişkin, bilgilendirilmeye dayanan ve özgür iradeyle açıklanan rıza.
İmha	Kişisel verilerin silinmesi, yok edilmesi veya anonim hale getirilmesi.
Kayıt Ortamı	Tamamen veya kısmen otomatik olan ya da herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla işlenen kişisel verilerin bulunduğu her türlü ortam.
Kişisel Veri	Kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgi.
Özel Nitelikli Kişisel Veri	Kişilerin ırkı, etnik kökeni, siyasi düşüncesi, felsefi inancı, dini, mezhebi veya diğer inançları, kılık ve kıyafeti, dernek, vakıf ya da sendika üyeliği, sağlığı, cinsel hayatı, ceza mahkûmiyeti ve güvenlik tedbirleriyle ilgili verileri ile biyometrik ve genetik verileri.
Kişisel Verilerin İşlenmesi	Kişisel verilerin tamamen veya kısmen otomatik olan ya da herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla elde edilmesi, kaydedilmesi, depolanması, muhafaza edilmesi, değiştirilmesi, yeniden düzenlenmesi, açıklanması, aktarılması, devralınması, elde edilebilir hâle getirilmesi, sınıflandırılması ya da kullanılmasının engellenmesi gibi veriler üzerinde gerçekleştirilen her türlü işlem.
Kişisel Verilerin Anonim Hale Getirilmesi	Kişisel verilerin, başka verilerle eşleştirilerek dahi hiçbir surette kimliği belirli veya belirlenebilir bir gerçek kişiyle ilişkilendirilemeyecek hâle getirilmesi.
Kişisel Verilerin Silinmesi	Kişisel verilerin silinmesi; kişisel verilerin ilgili kullanıcılar için hiçbir şekilde erişilemez ve tekrar kullanılamaz hale getirilmesi.

ABBREVIATIONS AND CONCEPTS

PPD Act	Protection of Personal Data Act No. 6698 published in the Official Journal no. 29677 dated 7 th April 2016
GDPR	EU (European Union) General Data Protection Regulation
Constitution	Constitution of the Republic of Turkey no. 2709 dated 7 th November 1982 published in the Official Journal no. 17863 dated 9 th November 1982
Data Processor	Person who is not included in the data controller's organisation and who processes the personal data in accordance with the powers and instructions received from the data controller, except the person or unit technically responsible for the storage, protection and backup of data.
Data Owner/ Related Person	Any natural person whose personal data are processed such as the employees, customers, business partners, shareholders, authorised officials, potential customers, candidate employees, trainees, visitors, suppliers of the COMPANY and/or the subsidiaries/ affiliates of the COMPANY who are included in the People/Related People who have business relationship with the former, employees of those corporations with which they cooperate, third parties and other people including but not limited to those listed herein.
Data Controller	Any natural person or legal entity who identifies the processing purposes and tools of personal data and who is responsible for the installation and management of the data recording system.
Explicit Consent	Consent concerning a particular issue, basing on information and disclosed in free will.
Destruction	Deletion, destruction or anonymization of personal data.
Recording Media	Any and all media containing personal data processed in a fully or partly automated manner or in a non-automatic manner provided that it is part of any data recording system.
Personal Data	Any and all data belonging to any identified or identifiable person.
Sensitive Personal Data	Any individual's data concerning his/her race, ethnical background, political view, philosophical belief, religion, creed or other faith, raiment, foundation or labour union membership, health, sexual life, criminal conviction and security measures as well as his/her genetic and biometric data.
Processing of Personal Data	Any and all operations carried out on data such as the obtaining, recording, storage, maintenance, modification, reorganisation, disclosure, transfer, takeover, making available, classification or prevention of use of personal data processed in a fully or partly automated manner or in a non-automatic manner provided that it is part of any data recording system.



PASETEL Ltd. Şti.
İzmir- TÜRKİYE

KİŞİSEL VERİLERİN KORUNMASI VE İŞLENMESİ, KİŞİSEL VERİ SAKLAMA VE İMHA POLİTİKASI

Protection, Processing Storage and Destruction of Personal Data Policy
Kod/Code # FR-03.40

Tarih / Date :

Sayfa / Page : 3 / 54

Kişisel Verilerin Yok Edilmesi	Kişisel verilerin hiç kimse tarafından hiçbir şekilde erişilemez, geri getirilemez ve tekrar kullanılamaz hale getirilmesi işlemi.
Periyodik İmha	Kanunda yer alan kişisel verilerin işleme şartlarının tamamının ortadan kalkması durumunda tekrar eden aralıklarla re'sen gerçekleştirilecek silme, yok etme veya anonim hale getirme işlemi.
Yönetmelik	28 Ekim 2017 tarihli 30224 sayılı Resmi Gazete'de yayımlanan ve 1 Ocak 2018 tarihi itibarıyla yürürlüğe giren Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmelik.
KVK Kurulu / Kurul	Kişisel Verileri Koruma Kurulu
KVK Kurumu	Kişisel Verileri Koruma Kurumu
Politika	PASETEL SİSTEM MÜH. SAN. ve TİC. LTD. ŞTİ. Şirketi Kişisel Verilerin Korunması Ve İşlenmesi Politikası
ŞİRKET	PASETEL SİSTEM MÜH. SAN. ve TİC. LTD. ŞTİ. Şirketi
Türk Ceza Kanunu	12 Ekim 2004 tarihli ve 25611 sayılı Resmi Gazete'de yayımlanan; 26 Eylül 2004 tarihli ve 5237 sayılı Türk Ceza Kanunu.

Destruction of Personal Data	Process of making personal data not accessible, retrievable nor re-usable in any manner whatsoever by any individuals.
Periodical Destruction	Process of deletion, destruction or anonymization which will be carried out in one's own initiative at recurring intervals in case the processing conditions of personal data as contained in the Act cease to exist in their entirety.
Regulation	Regulation Concerning the Deletion, Destruction or Anonymization of Personal Data published in the Official Journal no. 30224 dated 28 th October 2017, which became effective as of 1 st January 2018.
PPD Committee/ Committee	Protection of Personal Data Committee
PPD Authority	Protection of Personal Data Authority
Policy	Protection and Processing of Personal Data Policy of PASETEL SİSTEM MÜH. SAN. ve TİC. LTD. ŞTİ.
COMPANY	PASETEL SİSTEM MÜH. SAN. ve TİC. LTD. ŞTİ.
Turkish Criminal Code	Turkish Criminal Code No. 5237 dated 26 th September 2004, which was published in the Official Journal no. 25611 dated 12 th October 2004.

1. GİRİŞ

1.1. Amaç

Şirket olarak, anayasal bir hak olarak düzenlenen kişisel verilerin korunması ve hukuksal güvence altına alınması konusunda, sorumluluğumuzun farkındayız ve kişisel verilerinizin güvenli bir şekilde kullanımına önem veriyoruz.

Bu politikanın amacı ŞİRKET'in kişisel verileri 7 Nisan 2016 tarihli ve 29677 sayılı Resmi Gazete'de yayımlanmış olan Kişisel Verilerin Korunması Kanunu'na (KVKK) uyumlu bir şekilde işlenmesini ve korunmasını sağlamak için izlenecek yöntem ve ilkeleri düzenlemektir.

Bu şekilde Veri Sorumlusu tarafından gerçekleştirilen kişisel verilerin işlenmesi ve korunması faaliyetlerinde mevzuata tam uyumun sağlanması ve kişisel veri sahiplerinin kişisel verilere dair mevzuattan kaynaklanan tüm haklarının korunması hedeflenmektedir.

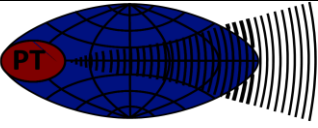
1. INTRODUCTION

1.1. Object

We, as a company, are aware of our responsibility for the protection and legal security of personal data which are regulated as a constitutional right and place importance on the safe use of your personal data.

The object of this policy is to regulate the methods and principles to be pursued by the COMPANY in order to ensure the processing and protection of personal data pursuant to the Protection of Personal Data Act (PPDA) published in the Official Journal No. 29677 dated 7th April 2016.

It is targeted to provide full compliance with the legislation and protect all rights related to personal data of the Data Owners arising from the legislation in the activities of processing and protecting personal data carried out in this way by the Data Controller.



PAGETEL Ltd. Şti.
İzmir- TÜRKİYE

KİŞİSEL VERİLERİN KORUNMASI VE İŞLENMESİ, KİŞİSEL VERİ SAKLAMA VE İMHA POLİTİKASI

Protection, Processing Storage and Destruction of Personal Data Policy
Kod/Code # FR-03.40

Tarih / Date :

Sayfa / Page : 4 / 54

1.2. Kapsam

Bu politika, ŞİRKET tarafından yönetilen, tüm kişisel verilerin işlenmesi ve korunmasına yönelik yürütülen faaliyetlerde uygulanmaktadır.

Bu politika; otomatik olan ya da herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla, Çalışan Adayı, Çalışan, Tedarikçi Yetkilisi, Ziyaretçi, Ürün veya Hizmet Alan Kişi, Tedarikçi Çalışanı, Potansiyel Ürün veya Hizmet Alıcısı, Dava, İcra Dosyası Tarafı, Tedarikçi, Kurumsal Müşteri Temsilcisi/Yetkilisi, Dış Hizmet Alımı Yapılan Firma Temsilcileri, Kamu Görevlisi, Müşteri Yetkilisi, Çalışan Yakını, Çalışan Adayı Referansı başta olmak üzere kişisel verileri Veri Sorumlusu tarafından işlenen gerçek kişileri kapsar. Bu Politika, hiçbir şekilde tüzel kişilere ve tüzel kişi verilerine uygulanmayacaktır.

Bu politika, ŞİRKET tarafından, tüm kişisel verilerin işlenmesi ve korunmasına yönelik yürütülen faaliyetlerde, ilgili detaylı veri prosedürleri ile birlikte uygulanmaktadır.

1.3. Politika'nın ve İlgili Mevzuatın Uygulanması

Kişisel verilerin işlenmesi ve korunması konusunda yürürlükte bulunan ilgili kanuni düzenlemeler öncelikle uygulama alanı bulacaktır. Yürürlükte bulunan mevzuat ve Politika arasında uyumsuzluk bulunması durumunda, Şirketimiz yürürlükteki mevzuatın uygulama alanı bulacağını kabul etmektedir.

1.4. Politika'nın Yürürlüğü

Şirketimiz tarafından düzenlenen bu Politika 09.10.2020 tarihlidir. Politika'nın tamamının veya belirli maddelerinin yenilenmesi durumunda Politika'nın yürürlük tarihi güncellenecektir.

Politika Şirketimizin internet sitesinde www.pagetel.com.tr yayımlanır ve kişisel veri sahiplerinin talebi üzerine ilgili kişilerin erişimine sunulur.

2. KİŞİSEL VERİLERİN KORUNMASINA İLİŞKİN HUSUSLAR

Şirketimiz, KVK Kanunu'nun 12. maddesine uygun olarak, işlemekte olduğu kişisel verilerin hukuka aykırı olarak işlenmesini önlemek, verilere hukuka aykırı olarak erişilmesini önlemek ve verilerin muhafazasını sağlamak için uygun güvenlik düzeyini sağlamaya yönelik gerekli teknik ve idari tedbirleri almakta, bu kapsamda gerekli denetimleri yapmak veya yaptırmaktadır.

1.2. Scope

This policy is applied in any activities conducted for the processing and protection of all personal data managed by the COMPANY.

This Policy covers any natural persons whose personal data are processed by the Data Controller including but not limited to Employee Candidates, Employees, Supplier's Authorised Officials, Visitors, Product or Service Purchasers, Supplier's Employees, Potential Product or Service Buyers, Litigants, Parties to Execution Files, Suppliers, Corporate Customer Representatives/Authorised Officials, Representatives of Companies from Which Exports Are Made, Public Officials, Customer's Authorised Officials, Employee's Kinsmen, Employee Candidate's References. This Policy shall not be applied to legal entities and legal entity data in any manner whatsoever.

This Policy is applied in any activities conducted for the processing and protection of all personal data together with any relevant detailed data procedures by the COMPANY.

1.3. Application of the Policy and the Relevant Legislation

Any legal regulations in effect which concern the processing and protection of personal data shall first find a field of application. The COMPANY agrees that in case there is any discrepancy between the legislation in effect and the Policy, the legislation in effect shall find a field of application.

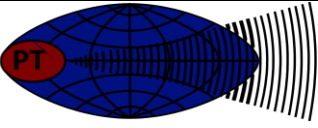
1.4. Effective Date of the Policy

This Policy drawn up by the COMPANY is dated 09.10.2020. In the event that all or certain articles of this Policy are renewed, the effective date of the Policy shall also be updated.

The Policy is published in the website of the COMPANY at www.pagetel.com.tr and presented to any relevant people for access upon the request of the personal data owners.

2. ISSUES CONCERNING THE PROTECTION OF PERSONAL DATA

The COMPANY takes any and all necessary technical and administrative measures in order to provide any proper security level to prevent illegal processing of the personal data which it is processing as per the article 12 of the PPD Act; to prevent any illegal access to such data; to ensure the maintenance of the data and carries out any necessary inspections in this context or cause the same to be carried out.



PAGETEL Ltd. Şti.
İzmir- TÜRKİYE

KİŞİSEL VERİLERİN KORUNMASI VE İŞLENMESİ, KİŞİSEL VERİ SAKLAMA VE İMHA POLİTİKASI

Protection, Processing Storage and Destruction of Personal Data Policy
Kod/Code # FR-03.40

Tarih / Date :

Sayfa / Page : 5 / 54

2.1. Kişisel Verilerin Güvenliğinin Sağlanması

2.1.1. Kişisel Verilerin Hukuka Uygun İşlenmesini Sağlamak, Hukuka Aykırı Erişimini Engellemek ve Güvenli Ortamlarda Saklanması İçin Alınan Teknik ve İdari Tedbirler

Şirketimiz, kişisel verilerin hukuka uygun işlenmesini sağlamak, bu verilerin hukuka aykırı erişimini engellemek ve güvenli ortamlarda saklanması için, teknolojik imkânlar ve uygulama maliyetine göre teknik ve idari tedbirler almaktadır.

2.1.1.1. Kişisel Verilerin Hukuka Uygun İşlenmesini Sağlamak, Hukuka Aykırı Erişimini Engellemek ve Güvenli Ortamlarda Saklanması İçin Alınan Teknik Tedbirler

Şirketimiz tarafından kişisel verilerin hukuka uygun işlenmesini sağlamak, bu verilerin hukuka aykırı erişimini engellemek ve güvenli ortamlarda saklanması için alınan başlıca teknik tedbirler aşağıda sıralanmaktadır:

- Ağ güvenliği ve uygulama güvenliği sağlanmaktadır
- Ağ yoluyla kişisel veri aktarımlarında kapalı sistem ağ kullanılmaktadır
- Anahtar yönetimi uygulanmaktadır
- Bilgi teknolojileri sistemleri tedarik, geliştirme ve bakımı kapsamındaki güvenlik önlemleri alınmaktadır
- Bulutta depolanan kişisel verilerin güvenliği sağlanmaktadır
- Erişim logları düzenli olarak tutulmaktadır
- Gerekliğinde veri maskeleyme önlemi uygulanmaktadır
- Güncel anti-virüs sistemleri kullanılmaktadır
- Güvenlik duvarları kullanılmaktadır
- Kişisel veriler yedeklenmekte ve yedeklenen kişisel verilerin güvenliği de sağlanmaktadır
- Kullanıcı hesap yönetimi ve yetki kontrol sistemi uygulanmakta olup bunların takibi de yapılmaktadır
- Log kayıtları kullanıcı müdahalesi olmayacak şekilde tutulmaktadır
- Özel nitelikli kişisel veriler elektronik posta yoluyla gönderilecekse mutlaka şifreli olarak ve KEP veya kurumsal posta hesabı kullanılarak gönderilmektedir
- Siber güvenlik önlemleri alınmış olup uygulanması sürekli takip edilmektedir
- Şifreleme yapılmaktadır
- Veri kaybı önleme yazılımları kullanılmaktadır
- Saldırı tespit ve önleme sistemleri kullanılmaktadır

2.1. Provision of the Security of Personal Data

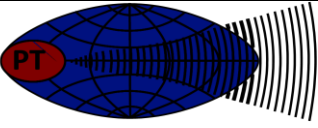
2.1.1. Technical and Administrative Measures Taken to Ensure Legal Processing of Personal Data; to Prevent Any Illegal Access to and Store the Data in Safe Media

The COMPANY takes technical and administrative measures on the basis of the technological opportunities and application costs in order to ensure legal processing of personal data; to prevent any illegal access thereto and store the data in safe media.

2.1.1.1. Technical Measures Taken to Ensure Legal Processing of Personal Data; to Prevent Any Illegal Access to and Store the Data in Safe Media

Basic technical measures taken to ensure legal processing of personal data; to prevent any illegal access thereto and store the data in safe media by the COMPANY are listed below:

- Network security and application security are provided.
- Closed system network is used in personal data transfers via network.
- Key management is conducted.
- Security measures are taken within the scope of the procurement, development and maintenance of information technology systems.
- Security of any personal data stored in Cloud is provided.
- Access logs are kept on regular basis.
- Data masking precaution is implemented when and if necessary.
- Current anti-virus systems are used.
- Security walls are used.
- Personal data are backed up and security of such backed up personal data is also provided.
- User account management and authorisation control system are conducted and they are tracked as well.
- Log entries are kept in a manner in which there will not be any user intervention.
- Sensitive personal data are absolutely sent in an encoded manner and using the Registered Electronic Mail (REM) or corporate mail account if they are to be sent via electronic mail.
- Cyber security measures have been taken and the implementation thereof is continuously tracked.
- Codification is made.
- Data loss prevention software is used.
- Attack identification and prevention systems are used.



PAGETEL Ltd. Şti.
Izmir- TÜRKİYE

KİŞİSEL VERİLERİN KORUNMASI VE İŞLENMESİ, KİŞİSEL VERİ SAKLAMA VE İMHA POLİTİKASI

Protection, Processing Storage and Destruction of Personal Data Policy
Kod/Code # FR-03.40

Tarih / Date :

Sayfa / Page : 6 / 54

2.1.1.2. Kişisel Verilerin Hukuka Uygun İşlenmesini Sağlamak, Hukuka Aykırı Erişimini Engellemek ve Güvenli Ortamlarda Saklanması İçin Alınan İdari Tedbirler

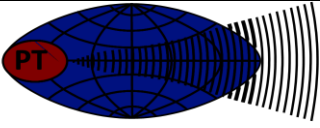
Şirketimiz tarafından kişisel verilerin hukuka uygun işlenmesini sağlamak, bu verilerin hukuka aykırı erişimini engellemek ve güvenli ortamlarda saklanması için alınan başlıca idari tedbirler aşağıda sıralanmaktadır:

- Çalışanlar için veri güvenliği hükümleri içeren disiplin düzenlemeleri mevcuttur
- Çalışanlar için veri güvenliği konusunda belli aralıklarla eğitim ve farkındalık çalışmaları yapılmaktadır
- Çalışanlar için yetki matrisi oluşturulmuştur
- Erişim, bilgi güvenliği, kullanım, saklama ve imha konularında kurumsal politikalar hazırlanmış ve uygulamaya başlanmıştır
- Gizlilik taahhütnameleri yapılmaktadır
- Görev değişikliği olan ya da işten ayrılan çalışanların bu alandaki yetkileri kaldırılmaktadır
- İmzalanan sözleşmeler veri güvenliği hükümleri içermektedir
- Kağıt yoluyla aktarılan kişisel veriler için ekstra güvenlik tedbirleri alınmakta ve ilgili evrak gizlilik dereceli belge formatında gönderilmektedir
- Kişisel veri güvenliği politika ve prosedürleri belirlenmiştir
- Kişisel veri güvenliği sorunları hızlı bir şekilde raporlanmaktadır
- Kişisel veri güvenliğinin takibi yapılmaktadır
- Kişisel veri içeren fiziksel ortamlara giriş çıkışlarla ilgili gerekli güvenlik önlemleri alınmaktadır
- Kişisel veri içeren fiziksel ortamların dış risklere (yangın, sel vb.) karşı güvenliği sağlanmaktadır
- Kişisel veri içeren ortamların güvenliği sağlanmaktadır
- Kişisel veriler mümkün olduğunca azaltılmaktadır
- Kurum içi periyodik ve/veya rastgele denetimler yapılmakta ve yaptırılmaktadır
- Mevcut risk ve tehditler belirlenmiştir
- Özel nitelikli kişisel veri güvenliğine yönelik protokol ve prosedürler belirlenmiş ve uygulanmaktadır
- Veri işleyen hizmet sağlayıcılarının veri güvenliği konusunda belli aralıklarla denetimi sağlanmaktadır
- Veri işleyen hizmet sağlayıcılarının, veri güvenliği konusunda farkındalığı sağlanmaktadır

2.1.1.2. Administrative Measures Taken to Ensure Legal Processing of Personal Data; to Prevent Any Illegal Access to and Store the Data in Safe Media

Basic administrative measures taken to ensure legal processing of personal data; to prevent any illegal access thereto and store the data in safe media by the COMPANY are listed below:

- There are available disciplinary regulations containing data security provisions for employees.
- Employees are provided with training and awareness studies on data security at regular intervals.
- An authorisation matrix has been created for employees.
- Corporate policies have been prepared and started to be implemented on access, information security, use, storage and destruction.
- Letters of commitment are drawn up for confidentiality.
- Authorisations of those employees who have change of position or who quit are removed in their respective fields.
- Contracts signed contain data security clauses.
- Extra security measures are taken for those data transferred in hardcopy and relevant documents are sent in "classified document" format.
- Personal data security policies and procedures have been identified.
- Personal data security issues are quickly reported.
- Personal data security is tracked.
- Any necessary security measures are taken for entries in and exits from any physical spaces containing personal data.
- Security of the physical spaces containing personal data is provided against external risks (fire, flood, etc.).
- Security of the physical spaces containing personal data is provided.
- Personal data are reduced as much as possible.
- In-house periodical and/or random audits are carried out or caused to be carried out.
- Any existing risks and threats have been identified.
- Protocols and procedures intended for sensitive personal data security have been identified and are implemented.
- Those service providers who process personal data are inspected with respect to data security at regular intervals.
- Those service providers who process personal data are ensured to have awareness on data security.



PAGETEL Ltd. Şti.
İzmir- TÜRKİYE

KİŞİSEL VERİLERİN KORUNMASI VE İŞLENMESİ, KİŞİSEL VERİ SAKLAMA VE İMHA POLİTİKASI

Protection, Processing Storage and Destruction of Personal Data Policy
Kod/Code # FR-03.40

Tarih / Date :

Sayfa / Page : 7 / 54

2.1.2. Kişisel Verilerin Korunması Konusunda Alınan Tedbirlerin Denetimi

Şirketimiz, KVK Kanunu'nun 12. maddesine uygun olarak, kendi bünyesinde gerekli denetimleri yapmakta veya yaptırmaktadır. Bu denetim sonuçları Şirketin iç işleyişi kapsamında konu ile ilgili bölüme raporlanmakta ve alınan tedbirlerin iyileştirilmesi için gerekli faaliyetler yürütülmektedir.

2.1.3. Kişisel Verilerin Yetkisiz Bir Şekilde İfşası Durumunda Alınacak Tedbirler

Şirketimiz, KVK Kanunu'nun 12. maddesine uygun olarak işlenen kişisel verilerin kanuni olmayan yollarla başkaları tarafından elde edilmesi halinde bu durumu en kısa sürede ilgili kişisel veri sahibine ve KVK Kurulu'na bildirilmesini sağlayan sistemi yürütmektedir.

2.2. Veri Sahibinin Haklarının Gözetilmesi; Bu Hakları Şirketimize İleteceği Kanalların Yaratılması ve Veri Sahiplerinin Taleplerinin Değerlendirmesi

Şirketimiz, kişisel veri sahiplerinin haklarının değerlendirilmesi ve kişisel veri sahiplerine gereken bilgilendirmenin yapılması için KVK Kanunu'nun 13. maddesine uygun olarak gerekli kanalları, iç işleyişi, idari ve teknik düzenlemeleri yürütmektedir.

2.1.2. Control of the Measures Taken for the Protection of Personal Data

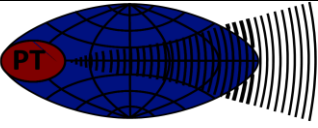
The COMPANY carries out any necessary controls or causes the same to be carried out within its own organisation as per the article 12 of the PPD Act. Results of such controls are reported to the department concerning the matter within the scope of the internal functioning of the COMPANY and activities necessary for the improvement of the measures taken are implemented.

2.1.3. Measures to Be Taken in Case of Unauthorised Disclosure of Personal Data

The COMPANY conducts the system which, if any personal data processed in accordance with the article 12 of the PPD Act are obtained through illegal ways by any other parties, ensures the relevant Personal Data Owner and the PPD Committee of the fact as soon as possible.

2.2. Observance of the Rights of the Data Owner; Creation of Channels by Which He/She Will Communicate Such Rights to the Company and Assessment of the Requests of Data Owners

The COMPANY conducts any necessary channels, internal functioning and technical and administrative arrangements pursuant to the article 13 of the PPD Act in order to assess the rights of the personal data owners and to provide the personal data owners with any necessary information.



PAGETEL Ltd. Şti.
İzmir- TÜRKİYE

KİŞİSEL VERİLERİN KORUNMASI VE İŞLENMESİ, KİŞİSEL VERİ SAKLAMA VE İMHA POLİTİKASI

Protection, Processing Storage and Destruction of Personal Data Policy
Kod/Code # FR-03.40

Tarih / Date :

Sayfa / Page : 8 / 54

Kişisel veri sahipleri aşağıda sıralanan haklarına ilişkin taleplerini yazılı olarak Şirketimize iletmeleri durumunda Şirketimiz talebin niteliğine göre talebi en kısa sürede ve en geç otuz gün içinde ücretsiz olarak sonuçlandırmaktadır. Ancak, işlemin ayrıca bir maliyeti gerektirmesi hâlinde, Şirketimiz tarafından KVK Kurulunca belirlenen tarifedeki ücret alınacaktır. Kişisel veri sahipleri;

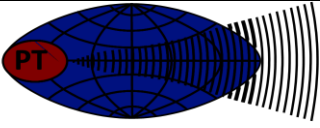
- Kişisel veri işlenip işlenmediğini öğrenme,
- Kişisel verileri işlenmişse buna ilişkin bilgi talep etme,
- Kişisel verilerin işlenme amacını ve bunların amacına uygun kullanılıp kullanılmadığını öğrenme,
- Yurt içinde veya yurt dışında kişisel verilerin aktarıldığı üçüncü kişileri bilme,
- Kişisel verilerin eksik veya yanlış işlenmiş olması hâlinde bunların düzeltilmesini isteme ve bu kapsamda yapılan işlemin kişisel verilerin aktarıldığı üçüncü kişilere bildirilmesini isteme,
- KVK Kanunu ve ilgili diğer kanun hükümlerine uygun olarak işlenmiş olmasına rağmen, işlenmesini gerektiren sebeplerin ortadan kalkması hâlinde kişisel verilerin silinmesini veya yok edilmesini isteme ve bu kapsamda yapılan işlemin kişisel verilerin aktarıldığı üçüncü kişilere bildirilmesini isteme,
- İşlenen verilerin münhasıran otomatik sistemler vasıtasıyla analiz edilmesi suretiyle kişinin kendisi aleyhine bir sonucun ortaya çıkmasına itiraz etme,
- Kişisel verilerin kanuna aykırı olarak işlenmesi sebebiyle zarara uğraması hâlinde zararın giderilmesini talep etme, haklarına sahiptir.

Veri sahiplerinin hakları ile ilgili daha ayrıntılı bilgiye bu Politika'nın 10. Bölümünde yer verilmiştir.

In case the personal data owners communicate their requests related to their rights as listed below to the COMPANY in a written form, the COMPANY concludes such request on free of charge basis as soon as possible but not later than thirty days depending on the nature of the request. However, in case the operation requires an extra cost, then the COMPANY shall charge the fee as fixed by the PPD Committee. Personal data owners have the right

- to learn whether or not their personal data are processed;
- if their personal data have been processed, to request information thereon;
- to learn the purpose of processing their personal data and whether or not such data are used to the purpose;
- to know any third parties to whom their personal data are transferred at home and abroad;
- in case their personal data have been deficiently or erroneously processed, to require the same to be corrected and to request that the action taken to that effect is to be notified to the third parties to whom such data have been transferred;
- in case the reasons for the processing of their personal data cease to exist –even though they have been processed pursuant to the PPD Act and any other relevant legal provisions, to require their personal data to be deleted or destroyed and to request the action taken to that effect to be notified to the third parties to whom such data have been transferred;
- to raise objection to the emergence of any outcome against the person himself/herself by solely analysing the processed data via automated systems;
- in case they incur losses due to illegal processing of their personal data, to require their losses to be compensated.

More detailed information concerning the rights of data owners is provided in Section 10 of this Policy.



PAGETEL Ltd. Şti.
İzmir- TÜRKİYE

KİŞİSEL VERİLERİN KORUNMASI VE İŞLENMESİ, KİŞİSEL VERİ SAKLAMA VE İMHA POLİTİKASI

Protection, Processing Storage and Destruction of Personal Data Policy
Kod/Code # FR-03.40

Tarih / Date :

Sayfa / Page : 9 / 54

2.3. Özel Nitelikli Kişisel Verilerin Korunması

KVK Kanunu ile bir takım kişisel verilere, hukuka aykırı olarak işlenmesi durumunda kişilerin mağduriyetine veya ayrımcılığa sebep olma riski nedeniyle özel önem atfedilmiştir.

Bu veriler; ırk, etnik köken, siyasi düşünce, felsefi inanç, din, mezhep veya diğer inançlar, kılık ve kıyafet, dernek, vakıf ya da sendika üyeliği, sağlık, cinsel hayat, ceza mahkûmiyeti ve güvenlik tedbirleriyle ilgili veriler ile biyometrik ve genetik verilerdir.

Şirketimiz tarafından, KVK Kanunu ile "özel nitelikli" olarak belirlenen ve hukuka uygun olarak işlenen özel nitelikli kişisel verilerin korunmasında hassasiyetle davranılmaktadır. Bu kapsamda, Şirketimiz tarafından, kişisel verilerin korunması için alınan teknik ve idari tedbirler, özel nitelikli kişisel veriler bakımından özenle uygulanmakta ve ŞİRKET bünyesinde gerekli denetimler sağlanmaktadır.

Şirket, Kanun'un 6. Maddesinde yer alan, Özel Nitelikli Kişisel Veriler'in işlenmesinde, Kurul'un 31.01.2018 Tarihli ve 2018/10 Numaralı kararı uyarınca, veri sorumlusu sıfatıyla, aşağıda belirtilen önlemleri almaktadır:

- Özel nitelikli kişisel verilerin güvenliğine yönelik sistemli, kuralları net bir şekilde belli, yönetilebilir ve sürdürülebilir işbu Politika belirlenmiştir.
- Özel nitelikli kişisel verilerin işlenmesi süreçlerinde yer alan Çalışan'lara yönelik,
 - Kanun ve buna bağlı yönetmelikler ile Özel Nitelikli Kişisel Veri güvenliği konularında düzenli olarak eğitimler verilmektedir,
 - Gizlilik sözleşmeleri yapılmaktadır,
 - Verilere erişim yetkisine sahip kullanıcıların, yetki kapsamı ve süreleri net olarak tanımlanmaktadır,
 - Periyodik olarak yetki kontrolleri gerçekleştirilmektedir,
 - Görev değişikliği olan ya da işten ayrılan Çalışanlar'ın bu alandaki yetkileri derhal kaldırılmaktadır. Bu kapsamda, Veri Sorumlusu tarafından kendisine tahsis edilen envanteri iade almaktadır.

2.3. Protection of Sensitive Personal Data

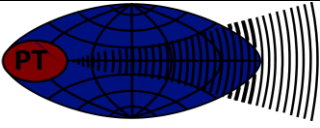
By the PPD Act, special importance is attributed to some personal data due to the risk of causing suffering or discrimination of people in case they are processed in an illegal manner.

Such data are those related to race, ethnical background, political view, philosophical belief, religion, creed or other faith, raiment, foundation or labour union membership, health, sexual life, criminal conviction and security measures as well as genetic and biometric data.

The COMPANY behaves in a sensitive manner in the protection of the sensitive personal data identified to be "sensitive" data and processed pursuant to the Act. In this context, Technical and administrative measures taken for the protection of personal data by the COMPANY are carefully applied with respect to sensitive personal data and any necessary controls are provided within the COMPANY.

The COMPANY, in its capacity as the Data Controller, takes the following measures in the processing of the Sensitive Personal Data as contained in the article 6 of the Act as per the Committee's decision no. 2018/1 of 31.01.2018:

- This systematic, manageable and sustainable Policy with clearly defined rules for the security of the sensitive personal data has been determined.
- For those Employees who participate in the processes of processing sensitive personal data,
 - regular trainings are provided on the security of the Sensitive Personal Data under the Act and regulations related thereto;
 - confidentiality contracts are executed;
 - authorisation extents and times of those users authorised to have access to the data are clearly identified;
 - authorisation checks are carried out at regular intervals;
 - of those Employees who change their positions or who quit their jobs, powers in such fields are immediately revoked. In this context, they return the inventory allocated to them by the Data Controller.



PAGETEL Ltd. Şti.
İzmir- TÜRKİYE

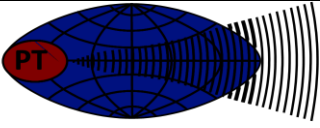
KİŞİSEL VERİLERİN KORUNMASI VE İŞLENMESİ, KİŞİSEL VERİ SAKLAMA VE İMHA POLİTİKASI

Protection, Processing Storage and Destruction of Personal Data Policy
Kod/Code # FR-03.40

Tarih / Date :

Sayfa / Page : 10 /
54

- Özel Nitelikli Kişisel Verilerin işlendiği, muhafaza edildiği ve/veya erişildiği ortamlar, elektronik ortam ise,
 - Kişisel Veriler üzerinde gerçekleştirilen tüm hareketlerin işlem kayıtları güvenli olarak loglanmaktadır,
 - Kişisel Veriler'in bulunduğu ortamlara ait güvenlik güncellemelerinin sürekli takip edilmekte, gerekli güvenlik testleri düzenli olarak yapılmakta/yaptırılmakta, test sonuçları kayıt altına alınmaktadır,
 - Kişisel Veriler'e bir yazılım aracılığı ile erişiliyorsa bu yazılıma ait kullanıcı yetkilendirmeleri yapılmakta, bu yazılımların güvenlik testleri düzenli olarak yapılmakta/yaptırılmakta, test sonuçları kayıt altına alınmaktadır,
- Özel Nitelikli Kişisel Verilerin işlendiği, muhafaza edildiği ve/veya erişildiği ortamlar, fiziksel ortam ise;
 - Özel Nitelikli Kişisel Veriler'in bulunduğu ortamın niteliğine göre yeterli güvenlik önlemleri (elektrik kaçağı, yangın, su baskını, hırsızlık vb. durumlara karşı) alınmaktadır,
 - Bu ortamların fiziksel güvenliğinin sağlanarak yetkisiz giriş çıkışlar engellenmektedir.
- Özel Nitelikli Kişisel Veriler aktarılacaksa
 - Kişisel Verilerin e-posta yoluyla aktarılması gerekiyorsa şifreli olarak kurumsal e-posta adresiyle veya Kayıtlı Elektronik Posta (KEP) hesabı kullanılarak aktarılmaktadır,
 - 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 alınmaktadır.
- If the media in which any Sensitive Personal Data are processed, stored and/or accessed are electronic media,
 - Operational records of all actions taken on Personal data are securely logged.
 - Security updates belonging to the media in which Personal Data are contained are continuously tracked, necessary security tests are continuously performed/caused to be performed, and test results are recorded.
 - If Personal Data are accessed via any software, user authorisations for such software are granted; security tests are regularly performed/caused to be performed on such software and test results are recorded.
- If the media in which Sensitive Personal Data re processed, stored and/or accessed are physical media,
 - adequate safety measures (electric leakage, fire, inundation, theft, etc.) are taken by the nature of the media in which such Sensitive Personal Data are contained;
 - physical security of such fields are provided and any unauthorised entries and exits are prevented.
- If Sensitive Personal Data are to be transferred,
 - if Personal Data are to be transferred via e-mail, they are transferred in an encoded manner via the corporate e-mail or by using the Registered Electronic Mail (REM) account;
 - any technical and administrative measures intended for the provision of the proper security level as stated in the website of the Protection of Personal Data Authority are taken into consideration as well as those measures mentioned above.



PAGETEL Ltd. Şti.
İzmir- TÜRKİYE

KİŞİSEL VERİLERİN KORUNMASI VE İŞLENMESİ, KİŞİSEL VERİ SAKLAMA VE İMHA POLİTİKASI

Protection, Processing Storage and Destruction of Personal Data Policy
Kod/Code # FR-03.40

Tarih / Date :

Sayfa / Page : 11 /
54

2.4. İş Birimlerinin Kişisel Verilerin Korunması ve İşlenmesi Konusunda Farkındalıklarının Artırılması ve Denetimi

Şirketimiz, kişisel verilerin hukuka aykırı olarak işlenmesini, verilere hukuka aykırı olarak erişilmesini önlemeye ve verilerin muhafazasını sağlamaya yönelik farkındalığın artırılması için iş birimlerine gerekli eğitimlerin düzenlenmesini sağlamaktadır.

Şirketin iş birimlerinin mevcut çalışanlarının ve iş birimi bünyesine yeni dâhil olmuş çalışanların kişisel verilerin korunması konusunda farkındalığının oluşması için gerekli sistemler kurulmakta, konuya ilişkin ihtiyaç duyulması halinde profesyonel kişiler ile çalışılmaktadır.

Şirketin iş birimlerinin kişisel verilerin korunması ve işlenmesi konusunda farkındalığın artırılmasına yönelik yürütülen eğitim sonuçları Şirkete raporlanmaktadır. Şirketimiz bu doğrultuda ilgili eğitimlere, seminerlere ve bilgilendirme oturumlarına yapılan katılımları değerlendirmekte ve gerekli denetimleri yapmakta veya yaptırmaktadır. Şirketimiz, ilgili mevzuatın güncellenmesine paralel olarak eğitimlerini güncellemekte ve yenilemektedir.

3. KİŞİSEL VERİLERİN İŞLENMESİNE İLİŞKİN HUSUSLAR

Şirketimiz, Anayasa'nın 20. maddesine ve KVK Kanunu'nun 4. maddesine uygun olarak, kişisel verilerin işlenmesi konusunda; hukuka ve dürüstlük kurallarına uygun; doğru ve gerektiğinde güncel; belirli, açık ve meşru amaçlar güderek; amaçla bağlantılı, sınırlı ve ölçülü bir biçimde kişisel veri işleme faaliyetinde bulunmaktadır. Şirketimiz kanunlarda öngörülen veya kişisel veri işleme amacının gerektirdiği süre kadar kişisel verileri muhafaza etmektedir.

Şirketimiz, Anayasa'nın 20. ve KVK Kanunu'nun 5. maddeleri gereğince, kişisel verileri, kişisel verilerin işlenmesine ilişkin KVK Kanunu'nun 5. maddesindeki şartlardan bir veya birkaçına dayalı olarak işlemektedir.

Şirketimiz, Anayasa'nın 20. ve KVK Kanunu'nun 10. maddelerine uygun olarak, kişisel veri sahiplerini aydınlatmakta ve kişisel veri sahiplerinin bilgi talep etmeleri durumunda gerekli bilgilendirmeyi yapmaktadır.

Şirketimiz, KVK Kanunu'nun 6. maddesine uygun olarak özel nitelikli kişisel verilerin işlenmesi bakımından öngörülen düzenlemelere uygun hareket etmektedir.

2.4. Enhancement and Control of Awareness on the Protection and Processing of Personal Data of Business Units

The COMPANY ensures the organisation of any necessary trainings for business units in order to enhance the awareness for the prevention of illegal access to and illegal processing of personal data and for the provision of the maintenance of data.

Any necessary systems are installed in order to create awareness on the protection of the personal data of the existing employees of the business units of the COMPANY and of those employees who have recently joined the business units and professional individuals are worked with in case of need in the matter.

Outcomes of the trainings conducted for the enhancement of awareness on the protection and processing of personal data by the business units of the COMPANY are reported to the COMPANY. The COMPANY evaluates attendance to any relevant trainings, seminars and information sessions in this context and carries out any necessary audits or causes the same to be carried out. The COMPANY updates and renews its trainings in line with the updating of the relevant legislation.

3. ISSUES CONCERNING THE PROCESSING OF PERSONAL DATA

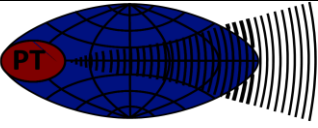
The COMPANY pursues a legal and fair, correct and -when necessary- current, specific, clear and legitimate purposes for the processing of personal data pursuant to the article 20 of the Constitution and the article 4 of the PPD Act and carries out personal data processing activities in a purpose-related, limited and moderate manner.

The COMPANY maintains personal data for a period as prescribed by laws or required by the purpose of processing personal data.

The COMPANY processes personal data on the basis of one or more of the conditions as contained in the article 5 of the PPD Act concerning the processing of personal data as per the article 20 of the Constitution and the article 5 of the PPD Act.

The COMPANY provides the personal data owners with clarification pursuant to the article 20 of the Constitution and the article 10 of the PPD Act and provides them with any necessary information in case any personal data owners request information.

The COMPANY acts in compliance with the anticipated regulations in terms of the processing of sensitive personal data pursuant to the article 6 of the PPD Act.



PAGETEL Ltd. Şti.
İzmir- TÜRKİYE

KİŞİSEL VERİLERİN KORUNMASI VE İŞLENMESİ, KİŞİSEL VERİ SAKLAMA VE İMHA POLİTİKASI

Protection, Processing Storage and Destruction of Personal Data Policy
Kod/Code # FR-03.40

Tarih / Date :

Sayfa / Page : 12 /
54

3.1. Kişisel Verilerin Mevzuatta Öngörülen İlkelerle Uygun Olarak İşlenmesi

3.1.1. Hukuka ve Dürüstlük Kuralına Uygun İşleme

Şirketimiz; kişisel verilerin işlenmesinde hukuksal düzenlemelerle getirilen ilkeler ile genel güven ve dürüstlük kuralına uygun hareket etmektedir. Bu kapsamda Şirketimiz, kişisel verilerin işlenmesinde orantılılık gerekliliklerini dikkate almakta, kişisel verileri amacı dışında kullanmamaktadır.

3.1.2. Kişisel Verilerin Doğru ve Gerekliğinde Güncel Olmasını Sağlama

Şirketimiz; kişisel veri sahiplerinin temel haklarını ve kendi meşru menfaatlerini dikkate alarak işlediği kişisel verilerin doğru ve güncel olmasını sağlamaktadır. Bu doğrultuda gerekli tedbirler almaktadır.

3.1.3. Belirli, Açık ve Meşru Amaçlarla İşleme

Şirketimiz, meşru ve hukuka uygun olan kişisel veri işleme amacını açık ve kesin olarak belirlemektedir. Şirketimiz, kişisel verileri sunmakta olduğu hizmetle bağlantılı ve bunlar için gerekli olan kadar işlemektedir. Şirketimiz tarafından kişisel verilerin hangi amaçla işleneceği henüz kişisel veri işleme faaliyeti başlamadan ortaya konulmaktadır.

3.1.4. İşlendikleri Amaçla Bağlantılı, Sınırlı ve Ölçülü Olma

Şirketimiz, kişisel verileri belirlenen amaçların gerçekleştirilmesine elverişli bir biçimde işlemekte ve amacın gerçekleştirilmesiyle ilgili olmayan veya ihtiyaç duyulmayan kişisel verilerin işlenmesinden kaçınmaktadır.

3.1. Processing of Personal Data in Compliance with the Principles Stipulated in Legislation

3.1.1. Processing in Compliance with Law and Good Faith

The COMPANY acts in compliance with any principles imposed by legal regulations and with the general rule of confidence and good faith in the processing of personal data. In this context, the COMPANY takes into consideration the proportionality requirements in the processing of personal data and does not misuse personal data.

3.1.2. Ensuring Personal Data to Be Correct and -When Necessary- Current

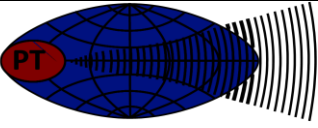
The COMPANY ensures any personal data which it processes to be correct and current in consideration of the basic rights of the data owners and its own legitimate interests. It takes any necessary measures to that effect.

3.1.3. Processing for Specific, Clear and Legitimate Purposes

The COMPANY clearly and specifically identifies its purpose of processing personal data in a legitimate and legal manner. The COMPANY processes personal data to the extent that they are related to the service it provides and that they are required for this purpose. The COMPANY reveals for what purposes personal data are to be processed before the commencement of the personal data processing activity.

3.1.4. Being Related to Their Purpose of Processing, Limited and Moderate

The COMPANY processes personal data in a manner which is eligible for achieving the identified purposes and avoids processing any personal data that are not related to the achievement of the purpose or that are not needed.



PAGETEL Ltd. Şti.
İzmir- TÜRKİYE

KİŞİSEL VERİLERİN KORUNMASI VE İŞLENMESİ, KİŞİSEL VERİ SAKLAMA VE İMHA POLİTİKASI

Protection, Processing Storage and Destruction of Personal Data Policy
Kod/Code # FR-03.40

Tarih / Date :

Sayfa / Page : 13 /
54

3.1.5. İlgili Mevzuatta Öngörülen veya İşlendikleri Amaç İçin Gerekli Olan Süre Kadar Muhafaza Etme

Şirketimiz, kişisel verileri ancak ilgili mevzuatta belirtildiği veya işlendikleri amaç için gerekli olan süre kadar muhafaza etmektedir. Bu kapsamda, Şirketimiz öncelikle ilgili mevzuatta kişisel verilerin saklanması için bir süre öngörülüp öngörülmediğini tespit etmekte, bir süre belirlenmişse bu süreye uygun davranmakta, bir süre belirlenmemişse kişisel verileri işlendikleri amaç için gerekli olan süre kadar saklamaktadır. Sürenin bitimi veya işlenmesini gerektiren sebeplerin ortadan kalkması halinde kişisel veriler Şirketimiz tarafından silinmekte, yok edilmekte veya anonim hale getirilmektedir. Gelecekte kullanma ihtimali ile Şirketimiz tarafından kişisel veriler saklanmamaktadır. Bu konu ile ilgili ayrıntılı bilgiye, bu Politika'nın 9. Bölümünde yer verilmiştir.

3.2. Kişisel Verilerin, KVK Kanunu'nun 5. Maddesinde Belirtilen Kişisel Veri İşleme Şartlarından Bir veya Birkaçına Dayalı ve Bu Şartlarla Sınırlı Olarak İşleme

Kişisel verilerin korunması Anayasal bir haktır. Temel hak ve hürriyetler, özlerine dokunulmaksızın yalnızca Anayasa'nın ilgili maddelerinde belirtilen sebeplere bağlı olarak ve ancak kanunla sınırlanabilir. Anayasa'nın 20. maddesinin üçüncü fıkrası gereğince, kişisel veriler ancak kanunda öngörülen hallerde veya kişinin açık rızasıyla işlenebilecektir. Şirketimiz bu doğrultuda ve Anayasa'ya uygun bir biçimde; kişisel verileri, ancak kanunda öngörülen hallerde veya kişinin açık rızasıyla işlemektedir. Bu konu ile ilgili ayrıntılı bilgiye, bu Politika'nın 7. Bölümünde yer verilmiştir.

3.3. Kişisel Veri Sahibinin Aydınlatılması ve Bilgilendirilmesi

Şirketimiz, KVK Kanunu'nun 10. maddesine uygun olarak, kişisel verilerin elde edilmesi sırasında kişisel veri sahiplerini aydınlatmaktadır. Bu kapsamda Şirket ve varsa temsilcisinin kimliğini, kişisel verilerin hangi amaçla işleneceğini, işlenen kişisel verilerin kimlere ve hangi amaçla aktarılacağı, kişisel veri toplamanın yöntemi ve hukuki sebebi ile kişisel veri sahibinin sahip olduğu hakları konusunda aydınlatma yapmaktadır. Bu konu ile ilgili ayrıntılı bilgiye bu Politika'nın 10. Bölümünde yer verilmiştir.

3.1.5. Maintaining Personal Data for the Period as Prescribed by the Relevant Legislation or Required for the Purposes of Processing

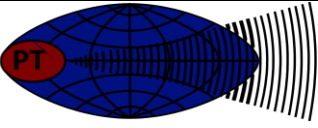
The COMPANY only maintains personal data for the period as prescribed in the relevant legislation or required for their purpose of processing. In this context, the COMPANY first determines whether or not any period of time has been fixed for the storage of personal data in the relevant legislation, observes such period if it has been fixed and stores personal data for the period as required for their purpose of processing. In case the period expires or if the reasons requiring them to be processed cease to exist, personal data are deleted, destroyed or anonymized by the COMPANY. The COMPANY would not store personal data, considering that they may be used in the future. Detailed information on the matter is provided in Section 9 of this Policy.

3.2. Processing Personal Data on the Basis of One or More of the Conditions as Stipulated in the Article 5 of the PPD Act and in a Manner Which Is Limited to Those Conditions

Protection of personal data is a constitutional right. Basic rights and freedoms may only be limited depending on the reasons set forth in the relevant articles of the Constitution and by law without tampering with their essence. As per the third paragraph of the article 20 of the Constitution, personal data may only be processed in any cases as stipulated in the Act or with the explicit consent of the relevant person. The COMPANY processes personal data only in the cases as stipulated by the Act or with the explicit consent of the relevant person in this context and pursuant to the Constitution. Detailed information on the matter is provided in Section 7 of this Policy.

3.3. Clarification of and Notification to Personal Data Owner

The COMPANY clarifies the personal data owners at the time of the obtaining of personal data pursuant to the article 10 of the PPD Act. In this context, the COMPANY provides clarification on the identity of the COMPANY and its representative (if any), for what purpose personal data will be processed, to who personal data will be transferred and for what purpose, the method and legal reason of collecting personal data and the rights which the personal data owner has. Detailed information on the matter is provided in Section 10 of this Policy.



PAGETEL Ltd. Şti.
İzmir- TÜRKİYE

KİŞİSEL VERİLERİN KORUNMASI VE İŞLENMESİ, KİŞİSEL VERİ SAKLAMA VE İMHA POLİTİKASI

Protection, Processing Storage and Destruction of Personal Data Policy
Kod/Code # FR-03.40

Tarih / Date :

Sayfa / Page : 14 /
54

Anayasa'nın 20. maddesinde herkesin, kendisiyle ilgili kişisel veriler hakkında bilgilendirilme hakkına sahip olduğu ortaya konulmuştur. Bu doğrultuda KVK Kanunu'nun 11. maddesinde kişisel veri sahibinin hakları arasında "bilgi talep etme" de sayılmıştır. Şirketimiz bu kapsamda, Anayasa'nın 20. ve KVK Kanunu'nun 11. maddelerine uygun olarak kişisel veri sahibinin bilgi talep etmesi durumunda gerekli bilgilendirmeyi yapmaktadır. Bu konu ile ilgili ayrıntılı bilgiye bu Politika'nın 10. Bölümünde yer verilmiştir.

3.4. Özel Nitelikli Kişisel Verilerin İşlenmesi

Şirketimiz tarafından, KVK Kanunu ile "özel nitelikli" olarak belirlenen kişisel verilerin işlenmesinde, KVK Kanunu'nda öngörülen düzenlemelere hassasiyetle uygun davranılmaktadır.

KVK Kanunu'nun 6. maddesinde, hukuka aykırı olarak işlendiğinde kişilerin mağduriyetine veya ayrımcılığa sebep olma riski taşıyan bir takım kişisel veri "özel nitelikli" olarak belirlenmiştir. Bu veriler; ırk, etnik köken, siyasi düşünce, felsefi inanç, din, mezhep veya diğer inançlar, kılık ve kıyafet, dernek, vakıf ya da sendika üyeliği, sağlık, cinsel hayat, ceza mahkûmiyeti ve güvenlik tedbirleriyle ilgili veriler ile biyometrik ve genetik verilerdir.

KVK Kanunu'na uygun bir biçimde Şirketimiz tarafından; özel nitelikli kişisel veriler, KVK Kurulu tarafından belirlenecek olan yeterli önlemlerin alınması kaydıyla aşağıdaki durumlarda işlenmektedir:

- Kişisel veri sahibinin açık rızası var ise veya
- Kişisel veri sahibinin açık rızası yok ise;
 - Kişisel veri sahibinin sağlığı ve cinsel hayatı dışındaki özel nitelikli kişisel veriler, kanunlarda öngörülen hallerde,
 - Kişisel veri sahibinin sağlığına ve cinsel hayatına ilişkin özel nitelikli kişisel verileri ise ancak kamu sağlığının korunması, koruyucu hekimlik, tıbbi teşhis, tedavi ve bakım hizmetlerinin yürütülmesi, sağlık hizmetleri ile finansmanının planlanması ve yönetimi amacıyla, sır saklama yükümlülüğü altında bulunan kişiler veya yetkili kurum ve kuruluşlar tarafından işlenmektedir.

It is stipulated in the article 20 of the Constitution that everyone is entitled to be clarified on any personal data related to him/her. Accordingly, "requesting information" is also included in the rights of a personal data owner in the article 11 of the PPD Act. In this context, the COMPANY provides any necessary clarification in case a personal data owner requests information pursuant to the article 20 of the Constitution and article 11 of the PPD Act. Detailed information on the matter is provided in Section 10 of this Policy.

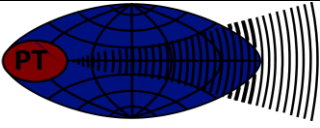
3.4. Processing of Sensitive Personal Data

The COMPANY acts in a sensitive manner in the processing of the personal data identified to be "sensitive" data in the PPD Act and any regulations as provided in the PPD Act.

In the article 6 of the PPD Act, some data bearing the risk of causing suffering or discrimination of people in case they are processed in an illegal manner are referred to as "sensitive data". Such data are those related to race, ethnical background, political view, philosophical belief, religion, creed or other faith, raiment, foundation or labour union membership, health, sexual life, criminal conviction and security measures as well as genetic and biometric data.

Sensitive personal data are processed in the following circumstances pursuant to the PPD Act by the COMPANY provided that any adequate measures to be identified by the PPD Committee are taken:

- if the personal data owner's explicit consent is available; or
- if the personal data owner's explicit consent is not available,
 - sensitive personal data other than the personal data owner's health and sexual life are processed in cases stipulated in laws;
 - sensitive personal data concerning the personal data owner's health and sexual life are only processed for the purposes of the protection of public health, implementation of preventive medicine, medical diagnosis, treatment and care services and planning and management of the healthcare services and financing thereof by those individuals or competent organisations or institutions obliged to keep secrets.



PAGETEL Ltd. Şti.
İzmir- TÜRKİYE

KİŞİSEL VERİLERİN KORUNMASI VE İŞLENMESİ, KİŞİSEL VERİ SAKLAMA VE İMHA POLİTİKASI

Protection, Processing Storage and Destruction of Personal Data Policy
Kod/Code # FR-03.40

Tarih / Date :

Sayfa / Page : 15 /
54

3.5. Kişisel Verilerin Aktarılması

Şirketimiz hukuka uygun olan kişisel veri işleme amaçları doğrultusunda gerekli güvenlik önlemlerini alarak (Bkz.2.1.) kişisel veri sahibinin kişisel verilerini ve özel nitelikli kişisel verilerini üçüncü kişilere aktarabilmektedir. Şirketimiz bu doğrultuda KVK Kanunu'nun 8. maddesinde öngörülen düzenlemelere uygun hareket etmektedir. Bu konu ile ilgili ayrıntılı bilgiye bu Politika'nın 6. Bölümünde yer verilmiştir.

3.5.1. Kişisel Verilerin Aktarılması

Şirketimiz meşru ve hukuka uygun kişisel veri işleme amaçları doğrultusunda aşağıda sayılan Kanunun 5. maddesinde belirtilen kişisel veri işleme şartlarından bir veya birkaçına dayalı ve sınırlı olarak kişisel verileri üçüncü kişilere aktarabilmektedir:

- Kişisel veri sahibinin açık rızası var ise;
- Kanunlarda kişisel verinin aktarılacağına ilişkin açık bir düzenleme var ise,
- Kişisel veri sahibinin veya başkasının hayatı veya beden bütünlüğünün korunması için zorunlu ise ve kişisel veri sahibi fiili imkânsızlık nedeniyle rızasını açıklayamayacak durumda ise veya rızasına hukuki geçerlilik tanınmıyorsa;
- Bir sözleşmenin kurulması veya ifasıyla doğrudan doğruya ilgili olmak kaydıyla sözleşmenin taraflarına ait kişisel verinin aktarılması gerekli ise,
- Şirketimizin hukuki yükümlülüğünü yerine getirmesi için kişisel veri aktarımı zorunlu ise,
- Kişisel veriler, kişisel veri sahibi tarafından alenileştirilmiş ise,
- Kişisel veri aktarımı bir hakkın tesisi, kullanılması veya korunması için zorunlu ise,
- Kişisel veri sahibinin temel hak ve özgürlüklerine zarar vermemek kaydıyla, Şirketimizin meşru menfaatleri için kişisel veri aktarımı zorunlu ise.

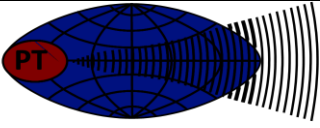
3.5. Transfer of Personal Data

The COMPANY may transfer the personal data and sensitive personal data of a personal data owner to any third parties in accordance with the legal purposes of processing personal data by taking any and all necessary security measures (see paragraph 2.1). In this context, the COMPANY acts in compliance with the regulations as stipulated in the article 8 of the PPD Act. Detailed information on the matter is provided in Section 6 of this Policy.

3.5.1. Transfer of Personal Data

The COMPANY may transfer personal data to any third parties basing on and limited to one or more of the personal data processing conditions as set forth in the article 5 of the Act and listed here below in accordance with the legitimate and legal personal data processing purposes:

- if the personal data owner's explicit consent is available;
- if there is any explicit regulation in the laws as to the fact that personal data may be transferred;
- if it is necessary for the protection of the life or physical integrity of the personal data owner or any other person and if the personal data owner is in a condition which prevents him/her from disclosing his/her explicit consent due to physical incapacity or his/her consent is not legally validated;
- if it is necessary to transfer the personal data of the contractual parties provided that it is directly related to the execution or performance of a contract;
- if transfer of personal data is necessary so that the COMPANY should fulfil its legal obligation;
- if personal data have been made public by the personal data owner;
- if transfer of personal data is necessary for the creation, exercise or protection of a right;
- if transfer of personal data is necessary for the COMPANY's legitimate interests provided that it will not prejudice the basic rights and freedoms of the personal data owner.



PAGETEL Ltd. Şti.
Izmir- TÜRKİYE

KİŞİSEL VERİLERİN KORUNMASI VE İŞLENMESİ, KİŞİSEL VERİ SAKLAMA VE İMHA POLİTİKASI

Protection, Processing Storage and Destruction of Personal Data Policy
Kod/Code # FR-03.40

Tarih / Date :

Sayfa / Page : 16 /
54

3.5.2. Özel Nitelikli Kişisel Verilerin Aktarılması

Şirketimiz gerekli özeni göstererek, gerekli güvenlik tedbirlerini alarak (Bkz. 2.1) ve KVK Kurulu tarafından öngörülen yeterli önlemleri alarak; meşru ve hukuka uygun kişisel veri işleme amaçları doğrultusunda kişisel veri sahibinin özel nitelikli verilerini aşağıdaki durumlarda üçüncü kişilere aktarabilmektedir.

- Kişisel veri sahibinin açık rızası var ise veya
- Kişisel veri sahibinin açık rızası yok ise;
 - Kişisel veri sahibinin sağlığı ve cinsel hayatı dışındaki özel nitelikli kişisel verileri (ırk, etnik köken, siyasi düşünce, felsefi inanç, din, mezhep veya diğer inançlar, kılık ve kıyafet, dernek, vakıf ya da sendika üyeliği, ceza mahkûmiyeti ve güvenlik tedbirleriyle ilgili veriler ile biyometrik ve genetik verilerdir), kanunlarda öngörülen hallerde,
 - Kişisel veri sahibinin sağlığına ve cinsel hayatına ilişkin özel nitelikli kişisel verileri ise ancak kamu sağlığının korunması, koruyucu hekimlik, tıbbi teşhis, tedavi ve bakım hizmetlerinin yürütülmesi, sağlık hizmetleri ile finansmanının planlanması ve yönetimi amacıyla, sır saklama yükümlülüğü altında bulunan kişiler veya yetkili kurum ve kuruluşlar tarafından.

3.6. Kişisel Verilerin Yurtdışına Aktarılması

Şirketimiz hukuka uygun kişisel veri işleme amaçları doğrultusunda gerekli güvenlik önlemleri alarak (Bkz. 2.1) kişisel veri sahibinin kişisel verilerini ve özel nitelikli kişisel verilerini üçüncü kişilere aktarabilmektedir.

Şirketimiz tarafından kişisel veriler; ilgili kişiden açık rıza alınması dışında; açık rıza alınmadan KVK Kurulu tarafından yeterli korumaya sahip olduğu ilan edilen yabancı ülkelere veya yeterli korumanın bulunmaması durumunda Türkiye'deki ve ilgili yabancı ülkedeki veri sorumlularının yeterli bir korumayı yazılı olarak taahhüt ettiği ve KVK Kurulu'nun izninin bulunduğu yabancı ülkelere ("Yeterli Korumayı Taahhüt Eden Veri Sorumlusunun Bulunduğu Yabancı Ülke") aktarılmaktadır. Şirketimiz bu doğrultuda KVK Kanunu'nun 9. maddesinde öngörülen düzenlemelere uygun hareket etmektedir.

3.5.2. Transfer of Sensitive Personal Data

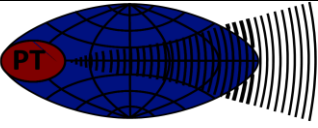
The COMPANY may transfer any sensitive personal data of a personal data owner to any third parties in accordance with its legitimate and legal personal data processing purposes in the following circumstances by taking any necessary care and taking any necessary security measures (see paragraph 2.1) and taking any adequate measures as prescribed by the PPD Committee.

- if the personal data owner's explicit consent is available; or
- if the personal data owner's explicit consent is not available,
 - sensitive personal data other than the personal data owner's health and sexual life (race, ethnical background, political view, philosophical belief, religion, creed or other faith, raiment, foundation or labour union membership, health, sexual life, criminal conviction and security measures as well as genetic and biometric data) are processed in cases stipulated in laws;
 - sensitive personal data concerning the personal data owner's health and sexual life are only processed for the purposes of the protection of public health, implementation of preventive medicine, medical diagnosis, treatment and care services and planning and management of the healthcare services and financing thereof by those individuals or competent organisations or institutions obliged to keep secrets.

3.6. Overseas Transfer of Personal Data

The COMPANY may transfer any personal data and sensitive personal data of a personal data owner to any third parties in accordance with its legitimate and legal personal data processing purposes by taking any necessary security measures (see paragraph 2.1).

Except in case of obtaining explicit consent of the relevant person, personal data are transferred to any foreign countries proclaimed to have adequate protection by the PPD Committee or –in case there is not adequate protection– to those foreign countries which the data controllers in Turkey or in any relevant foreign country undertake adequate protection in a written form and for which the PPD Committee permits ("Foreign Country Where a Data Controller Undertaking Adequate Protection Is Located") without obtaining explicit consent by the COMPANY. In this context, the COMPANY acts in compliance with the regulations as stipulated in the article 9 of the PPD Act.



PAGETEL Ltd. Şti.
İzmir- TÜRKİYE

KİŞİSEL VERİLERİN KORUNMASI VE İŞLENMESİ, KİŞİSEL VERİ SAKLAMA VE İMHA POLİTİKASI

Protection, Processing Storage and Destruction of Personal Data Policy
Kod/Code # FR-03.40

Tarih / Date :

Sayfa / Page : 17 /
54

3.6.1. Kişisel Verilerin Yurtdışına Aktarılması

Şirketimiz meşru ve hukuka uygun kişisel veri işleme amaçları doğrultusunda kişisel veri sahibinin açık rızası var ise veya kişisel veri sahibinin açık rızası yok ise aşağıdaki hallerden birinin varlığı durumunda kişisel verileri Yeterli Korumaya Sahip veya Yeterli Korumayı Taahhüt Eden Veri Sorumlusunun Bulunduğu Yabancı Ülkelere aktarabilmektedir:

- Kanunlarda kişisel verinin aktarılacağına ilişkin açık bir düzenleme var ise,
- Kişisel veri sahibinin veya başkasının hayatı veya beden bütünlüğünün korunması için zorunlu ise ve kişisel veri sahibi fiili imkânsızlık nedeniyle rızasını açıklayamayacak durumda ise veya rızasına hukuki geçerlilik tanınmıyorsa;
- Bir sözleşmenin kurulması veya ifasıyla doğrudan doğruya ilgili olmak kaydıyla sözleşmenin taraflarına ait kişisel verinin aktarılması gerekli ise,
- Şirketimizin hukuki yükümlülüğünü yerine getirmesi için kişisel veri aktarımı zorunlu ise,

3.6.2. Özel Nitelikli Kişisel Verilerin Yurtdışına Aktarılması

Şirketimiz gerekli özeni göstererek, gerekli güvenlik tedbirlerini alarak (Bkz. 2.1) ve KVK Kurulu tarafından öngörülen yeterli önlemleri alarak; meşru ve hukuka uygun kişisel veri işleme amaçları doğrultusunda kişisel veri sahibinin özel nitelikli verilerini aşağıdaki durumlarda Yeterli Korumaya Sahip veya Yeterli Korumayı Taahhüt Eden Veri Sorumlusunun Bulunduğu Yabancı Ülkelere aktarabilmektedir.

- Kişisel veri sahibinin açık rızası var ise veya
- Kişisel veri sahibinin açık rızası yok ise;
 - Kişisel veri sahibinin sağlığı ve cinsel hayatı dışındaki özel nitelikli kişisel verileri (ırk, etnik köken, siyasi düşünce, felsefi inanç, din, mezhep veya diğer inançlar, kılık ve kıyafet, dernek, vakıf ya da sendika üyeliği, ceza mahkûmiyeti ve güvenlik tedbirleriyle ilgili veriler ile biyometrik ve genetik verilerdir), kanunlarda öngörülen hallerde,
 - Kişisel veri sahibinin sağlığına ve cinsel hayatına ilişkin özel nitelikli kişisel verileri ise ancak kamu sağlığının korunması, koruyucu hekimlik, tıbbi teşhis, tedavi ve bakım hizmetlerinin yürütülmesi, sağlık hizmetleri ile finansmanının planlanması ve yönetimi amacıyla, sır saklama yükümlülüğü altında bulunan kişiler veya yetkili kurum ve kuruluşlar tarafından işlenmesi kapsamında aktarım yapılabilecektir.

3.6.1. Overseas Transfer of Personal Data

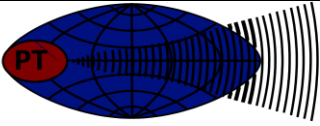
The COMPANY may transfer personal data to the Foreign Countries Having Adequate Protection or Where a Data Controller Undertaking Adequate Protection Is Located in case of the existence of the personal data owner's explicit consent or in case of the existence of any of the following conditions if the explicit consent of a personal data owner is not available:

- if there is an explicit provision in the relevant laws as to the fact that personal data are to be transferred;
- if it is necessary for the protection of the life or physical integrity of the personal data owner or any other person and if the personal data owner is in a condition which prevents him/her from disclosing his/her explicit consent due to physical incapacity or his/her consent is not legally validated;
- if it is necessary to transfer the personal data of the contractual parties provided that it is directly related to the execution or performance of a contract;
- if transfer of personal data is necessary so that the COMPANY should fulfil its legal obligation.

3.6.2. Overseas Transfer of Sensitive Personal Data

The COMPANY may transfer sensitive personal data of any personal data owner to the Foreign Countries Having Adequate Protection or Where a Data Controller Undertaking Adequate Protection Is by taking any necessary care and taking any necessary security measures (see paragraph 2.1) and taking any adequate measures as prescribed by the PPD Committee in the following conditions:

- if the personal data owner's explicit consent is available; or
- if the personal data owner's explicit consent is not available,
 - sensitive personal data other than the personal data owner's health and sexual life (race, ethnical background, political view, philosophical belief, religion, creed or other faith, raiment, foundation or labour union membership, health, sexual life, criminal conviction and security measures as well as genetic and biometric data) are processed in cases stipulated in laws;
 - sensitive personal data concerning the personal data owner's health and sexual life are only processed for the purposes of the protection of public health, implementation of preventive medicine, medical diagnosis, treatment and care services and planning and management of the healthcare services and financing thereof by those individuals or competent organisations or institutions obliged to keep secrets.



PAGETEL Ltd. Şti.
İzmir- TÜRKİYE

KİŞİSEL VERİLERİN KORUNMASI VE İŞLENMESİ, KİŞİSEL VERİ SAKLAMA VE İMHA POLİTİKASI

Protection, Processing Storage and Destruction of Personal Data Policy
Kod/Code # FR-03.40

Tarih / Date :

Sayfa / Page : 18 /
54

4. ŞİRKETİMİZ TARAFINDAN İŞLENEN KİŞİSEL VERİLERİN KATEGORİZASYONU, İŞLENME AMAÇLARI VE SAKLANMA SÜRELERİ

Şirketimiz, KVK Kanunu'nun 10. maddesine uygun olarak aydınlatma yükümlülüğü kapsamında hangi kişisel veri sahibi gruplarının kişisel verilerini işlediğini, kişisel veri sahibinin kişisel verilerinin işleme amaçlarını ve saklama sürelerini kişisel veri sahibine bildirmektedir.

4.1. Kişisel Verilerin Kategorizasyonu

Şirketimiz nezdinde, KVK Kanunu'nun 10. maddesi uyarınca ilgili kişiler bilgilendirilerek, Şirketimizin meşru ve hukuka uygun kişisel veri işleme amaçları doğrultusunda KVK Kanunu'nun 5. maddesinde belirtilen kişisel veri işleme şartlarından bir veya birkaçına dayalı ve sınırlı olarak KVK Kanunu'nda başta kişisel verilerin işlenmesine ilişkin 4. maddede belirtilen ilkeler olmak üzere KVK Kanunu'nda belirtilen genel ilkelere ve KVK Kanunu'nda düzenlenen bütün yükümlülüklerle uyararak işbu Politika kapsamındaki sùjelerle sınırlı olarak aşağıda belirtilen kategorilerdeki kişisel veriler işlenmektedir. Bu kategorilerde işlenen kişisel verilerin işbu Politika kapsamında düzenlenen hangi veri sahipleriyle ilişkili olduğu da işbu Politika'nın 5. Bölümünde belirtilmektedir.

Kişisel Veri Kategorizasyonu	Açıklama
Kimlik Bilgisi	Kimliği belirli veya belirlenebilir bir gerçek kişiye ait olduğu açık olan; kısmen veya tamamen otomatik şekilde veya veri kayıt sisteminin bir parçası olarak otomatik olmayan şekilde işlenen; kişinin kimliğine dair bilgilerin bulunduğu verilerdir; ad-soyad, T.C. kimlik numarası, uyruk bilgisi, anne adı-baba adı, doğum yeri, doğum tarihi, cinsiyet gibi bilgileri içeren ehliyet, nüfus cüzdanı ve pasaport gibi belgeler ile vergi numarası, SGK numarası, imza bilgisi, taşıt plakası v.b. bilgiler
İletişim Bilgisi	Kimliği belirli veya belirlenebilir bir gerçek kişiye ait olduğu açık olan; kısmen veya tamamen otomatik şekilde veya veri kayıt sisteminin bir parçası olarak otomatik olmayan şekilde işlenen; telefon numarası, adres, e-mail adresi, faks numarası, IP adresi gibi bilgiler
Özlük Bilgisi	Kimliği belirli veya belirlenebilir bir gerçek kişiye ait olduğu açık olan; kısmen veya tamamen otomatik şekilde veya veri kayıt sisteminin bir parçası olarak otomatik olmayan şekilde işlenen; Şirketimiz ile çalışma ilişkisi içerisinde olan gerçek kişilerin özlük haklarının oluşmasına temel olacak bilgilerin elde edilmesine yönelik işlenen her türlü kişisel veri

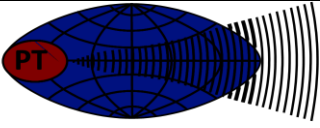
4. CATEGORISATION, PROCESSING PURPOSES AND STORAGE PERIODS OF PERSONAL DATA PROCESSED BY THE COMPANY

The COMPANY notifies the personal data owner of the personal data owner groups whose personal data it processes, purposes of processing the personal data of the personal data owner and the storage periods under its obligation to provide clarification pursuant to the article 10 of the PPD Act.

4.1. Categorisation of Personal Data

The COMPANY processes the personal data in the following categories limited to the subjects as contained in this Policy in accordance with the legitimate and legal personal data processing purposes of the COMPANY basing on and limited to one or more of the personal data processing conditions set forth in the article 5 of the PPD Act and complying with the general principles set forth in the PPD Act including but not limited to the article 4 concerning the processing of personal data and with any and all obligations as stipulated by the PPD Act by notifying any relevant people as per the article 10 of the PPD Act. To what data owners the personal data processed in such categories under this Policy are related is indicated in the Section 5 of this Policy.

Personal Data Categorisation	Description
Identity Information	Data apparently belonging to an identified or identifiable natural person, which are processed in a partly or completely automatic manner or in a non-automatic manner as part of a data recording system and which contain information about the identity of such person; such documents as driving license, identity card and passport containing such information as first name and last name, Turkish personal identity number, mother's name and father's name, place of birth, date of birth, gender, etc. and such information as tax identification number, social security number, signature, traffic license plate number, etc.
Contact Information	Such information as telephone number, residential address, e-mail address, facsimile number, IP address, etc. apparently belonging to an identified or identifiable natural person, which are processed in a partly or completely automatic manner or in a non-automatic manner as part of a data recording system.
Personal Information	Any personal data processed for the obtaining of any information which will be the basis of the formation of the personal rights of any natural persons who have business relations with the COMPANY and which apparently belongs to an identified or identifiable natural person, which are processed in a partly or completely automatic manner or in a non-automatic manner as part of a data recording system.



PAGETEL Ltd. Şti.
İzmir- TÜRKİYE

KİŞİSEL VERİLERİN KORUNMASI VE İŞLENMESİ, KİŞİSEL VERİ SAKLAMA VE İMHA POLİTİKASI

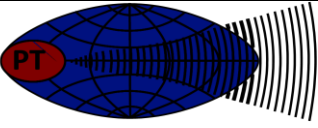
Protection, Processing Storage and Destruction of Personal Data Policy
Kod/Code # FR-03.40

Tarih / Date :

Sayfa / Page : 19 /
54

Hukuki İşlem ve Uyum Bilgisi	Şirket'in hukuki süreçleri, alacak ve haklarının tespiti, takibi ve borçlarının ifası ile kanuni yükümlülükleri kapsamında işlenen veriler, adli makamlarla yazışmalardaki bilgiler, gelen giden evraklar, dava dosyaları gibi bilgiler.
Müşteri İşlem Bilgisi	Kimliği belirli veya belirlenebilir bir gerçek kişiye ait olduğu açık olan, kısmen veya tamamen otomatik şekilde veya veri kayıt sisteminin bir parçası olarak otomatik olmayan şekilde işlenen; Şirket'in ticari faaliyetleri ve iş birimlerinin yürüttüğü operasyonlar neticesinde ilgili kişi hakkında elde edilen ve üretilen çağrı merkezi kayıtları, fatura, senet çek bilgisi, sipariş bilgisi, talep bilgisi, teklif, hizmet numarası gibi bilgiler.
Finansal Bilgi	Kimliği belirli veya belirlenebilir bir gerçek kişiye ait olduğu açık olan; kısmen veya tamamen otomatik şekilde veya veri kayıt sisteminin bir parçası olarak işlenen, Şirketimizin kişisel veri sahibi ile kurmuş olduğu hukuki ilişkinin tipine göre yaratılan her türlü finansal sonucu gösteren bilgi, belge ve kayıtlara ilişkin işlenen kişisel veriler ile banka hesap numarası, IBAN numarası, kredi kartı bilgisi, finansal profil, malvarlığı verisi, gelir bilgisi gibi veriler
Fiziksel Mekân Güvenlik Bilgisi	Kimliği belirli veya belirlenebilir bir gerçek kişiye ait olduğu açık olan; kısmen veya tamamen otomatik şekilde veya veri kayıt sisteminin bir parçası olarak işlenen; fiziksel mekana girişte, fiziksel mekanın içerisinde kalış sırasında alınan kayıtlar ve belgelere ilişkin kişisel veriler; kamera kayıtları, güvenlik noktasında alınan kayıtlar v.b.
Görsel/İşitsel Bilgi	Kimliği belirli veya belirlenebilir bir gerçek kişiye ait olduğu açık olan; fotoğraf ve kamera kayıtları (Fiziksel Mekan Güvenlik Bilgisi kapsamında giren kayıtlar hariç), ses kayıtları ile kişisel veri içeren belgelerin kopyası niteliğindeki belgelerde yer alan veriler
Ceza Mahkumiyeti Ve Güvenlik Tedbirleri Bilgileri	Kimliği belirli veya belirlenebilir bir gerçek kişiye ait olduğu açık olan; kısmen veya tamamen otomatik şekilde veya veri kayıt sisteminin bir parçası olarak otomatik olmayan şekilde işlenen; Şirket iş birimleri tarafından yürütülen operasyonlar çerçevesinde veya Şirket ile çalışma ilişkisi içerisinde olan gerçek kişilerin iş süreçlerini yürütmek veya Şirket'in ve Kişisel Veri Sahibi'nin hukuki ve diğer menfaatlerini korumak amacıyla elde edilen Kişisel Veri Sahibi'nin adli sicil kaydı gibi verileri
Risk Yönetimi Bilgileri	Kimliği belirli veya belirlenebilir bir gerçek kişiye ait olduğu açık olan; kısmen veya tamamen otomatik şekilde veya veri kayıt sisteminin bir parçası olarak otomatik olmayan şekilde işlenen; Şirket'in Kişisel Veri Sahibi ile kurmuş olduğu hukuki ilişkinin tipine göre yaratılan her türlü ticari, teknik, idari risklerin yönetilmesi için işlenen veriler.

Legal Proceeding and Compliance Information	Data processed within the scope of the legal processes of the COMPANY, identification and tracking of its claims and rights, performance of its liabilities and legal obligations, information contained in correspondence with judicial authorities, information such as incoming and outgoing documents, litigation files, etc.
Customer Transaction Information	Such information as call centre records, invoices, promissory notes, checks, purchase orders, demands, quotations, service number, etc. apparently belonging to an identified or identifiable natural person, which are processed in a partly or completely automatic manner or in a non-automatic manner as part of a data recording system, which are obtained or generated about people as a result of the business activities of the COMPANY and the operations carried out by its business units.
Financial Information	Personal data processed for any information, documentation and records showing any and all financial outcomes created by the type of the legal relationship which the COMPANY has established with the personal data owner as well as such data as the bank account number, IBAN, credit card, financial profile, assets, income, etc. which apparently belong to an identified or identifiable natural person, which are processed in a partly or completely automatic manner or in a non-automatic manner as part of a data recording system.
Physical Space and Security Information	Personal data concerning the records and documents taken at entrance to any physical spaces and during the stay in such physical space, camera recordings, records kept at the security point, etc., which apparently belong to an identified or identifiable natural person, which are processed in a partly or completely automatic manner or in a non-automatic manner as part of a data recording system.
Visual/Audio Information	Information contained in photographs and camera recordings (except any records as included in Physical Space Security Information), sound recordings and in any documents which are copies of documents containing personal data, which apparently belong to an identified or identifiable person.
Criminal Conviction and Security Measures Information	Personal Data Owner's criminal records obtained under the operations conducted by the business units of the COMPANY or in order to carry out business processes of any natural persons who have business relations with the COMPANY or to protect the legal and other interests of the Personal Data Owner, which apparently belong to an identified or identifiable natural person, which are processed in a partly or completely automatic manner or in a non-automatic manner as part of a data recording system.
Risk Management Information	Data apparently belonging to an identified or identifiable natural person and processed in a partly or completely automatic manner or in a non-automatic manner as part of a data recording system, which are created by the type of the legal relationship which the COMPANY has established with the Personal Data Owner and processed for the management of any and all commercial, technical and administrative risks.



PAGETEL Ltd. Şti.
Izmir- TÜRKİYE

KİŞİSEL VERİLERİN KORUNMASI VE İŞLENMESİ, KİŞİSEL VERİ SAKLAMA VE İMHA POLİTİKASI

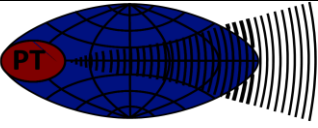
Protection, Processing Storage and Destruction of Personal Data Policy
Kod/Code # FR-03.40

Tarih / Date :

Sayfa / Page : 20 /
54

Sağlık Bilgileri	Kimliği belirli veya belirlenebilir bir gerçek kişiye ait olduğu açık olan; kısmen veya tamamen otomatik şekilde veya veri kayıt sisteminin bir parçası olarak otomatik olmayan şekilde işlenen; Şirket'in iş birimleri tarafından yürütülen operasyonlar çerçevesinde; sunduğu ürün ve hizmetlerle ilgili olarak veya Şirket ile çalışma ilişkisi içerisinde olan gerçek kişilerin iş süreçlerini yürütmek veya Şirket'in ve Kişisel Veri Sahibi'nin hukuki ve diğer menfaatlerini korumak amacıyla elde edilen Kişisel Veri Sahibi'nin ve/veya aile bireylerinin Sağlık Raporu, Engelli vergi muafiyet belgeleri, sigorta belgeleri, askerlik durum belgesi gibi sağlık verileri
İşlem Güvenliği Bilgisi	Şirket'in faaliyetlerini yürütürken, gerek Kişisel Veri Sahibi'nin gerekse de Şirket'in teknik, idari, hukuki ve ticari güvenliğine ilişkin işlenen IP Adres bilgileri, İnternet Sitesi giriş çıkış bilgileri, şifre ve parola bilgileri gibi kişisel veriler
Lokasyon Verisi	Kimliği belirli veya belirlenebilir bir gerçek kişiye ait olduğu açık olan; kısmen veya tamamen otomatik şekilde veya veri kayıt sisteminin bir parçası olarak otomatik olmayan şekilde işlenen; kişisel veri sahibinin iş birimleri tarafından yürütülen operasyonlar çerçevesinde, ürün ve hizmetlerinin kullanımı sırasında veya çalışanların araçlarını kullanırken bulunduğu yerin konumunu tespit eden bilgiler; GPS lokasyonu, seyahat verileri v.b.
Mesleki Deneyim Bilgisi	Kimliği belirli veya belirlenebilir bir gerçek kişiye ait olduğu açık olan; kısmen veya tamamen otomatik şekilde veya veri kayıt sisteminin bir parçası olarak otomatik olmayan şekilde, Şirket'in Kişisel Veri Sahibi ile kurmuş olduğu hukuki ilişkinin tipine göre işlenen; diploma bilgileri, gidilen kurslar, meslek içi eğitim bilgileri, sertifikalar, aday başvuru formları, referans görüşme bilgileri, iş görüşmesi bilgileri, transkript bilgileri gibi veriler.
Biyometrik Veri	avuç içi bilgileri, parmak izi bilgileri, retina taraması bilgileri, yüz tanıma bilgileri gibi
Araç Bilgisi	Araç Plakası
Çalışan Aile Bireyi ve Yakını Bilgisi	Eşinin Adı Soyadı, Çocukların Adı Soyadı, Çocukları Doğum Tarihi, Eşinin Doğum Tarihi, Çocuklarının Tc Nosu, Eşinin Tc Nosu, Anne-Baba TC Nosu

Medical Information	Such medical data as the medical reports, the handicapped tax exemption certificates, social security documents, military service certificates of the Personal Data Owner and/or the members of his/her family obtained under the operations conducted by the business units of the COMPANY or in connection with the products and services which the COMPANY supplies or in order to carry out business processes of any natural persons who have business relations with the COMPANY or to protect the legal and other interests of the Personal Data Owner, which apparently belong to an identified or identifiable natural person, which are processed in a partly or completely automatic manner or in a non-automatic manner as part of a data recording system.
Process Security Information	Such personal data as IP address information, website login/ logout information, password information processed for the technical, administrative and legal security of both the Personal Data Owner and the Company in the performance of the activities of the COMPANY.
Location Data	Such information as GPS location, travel data, etc. locating the position of the employees while using its products and services or driving its vehicles under the operations carried out by the business units of the personal data owner, which apparently belong to an identified or identifiable natural person, which are processed in a partly or completely automatic manner or in a non-automatic manner as part of a data recording system.
Professional Experience Information	Such data as diploma information, courses attended, on-the-job training information, certificates, candidate application forms, reference interview information, job interview information, transcript information, etc. apparently belonging to an identified or identifiable natural person, which are processed in a partly or completely automatic manner or in a non-automatic manner as part of a data recording system.
Biometric Data	Such information as palm print, finger print, retina scan, face recognition, etc.
Vehicle Information	Vehicle License Plate Number
Employee's Family Member and Kinsmen Information	Spouse's Full Name, Children's Full Names, Spouse's Birth Date, Children's Birth Dates, Spouse's Personal Identity Number, Children's Personal Identity Numbers, Parent's Personal Identity Numbers.



PAGETEL Ltd. Şti.
İzmir- TÜRKİYE

KİŞİSEL VERİLERİN KORUNMASI VE İŞLENMESİ, KİŞİSEL VERİ SAKLAMA VE İMHA POLİTİKASI

Protection, Processing Storage and Destruction of Personal Data Policy
Kod/Code # FR-03.40

Tarih / Date :

Sayfa / Page : 21 /
54

4.2. Kişisel Verilerin İşlenme Amaçları

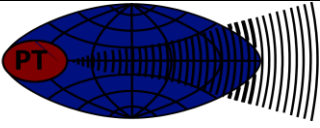
Şirketimiz, KVK Kanunu'nun 5. maddesinin 2. fıkrasında ve 6. maddenin 3. fıkrasında belirtilen kişisel veri işleme şartları içerisindeki amaçlarla ve koşullarla sınırlı olarak kişisel verileri işlemektedir. Bu amaçlar ve koşullar;

- Kişisel verilerinizin işlenmesine ilişkin Şirketin ilgili faaliyette bulunmasının Kanunlarda açıkça öngörülmesi
- Kişisel verilerinizin Şirket tarafından işlenmesinin bir sözleşmenin kurulması veya ifasıyla doğrudan doğruya ilgili ve gerekli olması
- Kişisel verilerinizin işlenmesinin Şirketin hukuki yükümlülüğünü yerine getirebilmesi için zorunlu olması
- Kişisel verilerinizin sizler tarafından alenileştirilmiş olması şartıyla; sizlerin alenileştirme amacıyla sınırlı bir şekilde Şirket tarafından işlenmesi
- Kişisel verilerinizin Şirket tarafından işlenmesinin Şirketin veya sizlerin veya üçüncü kişilerin haklarının tesisi, kullanılması veya korunması için zorunlu olması
- Sizlerin temel hak ve özgürlüklerine zarar vermemek kaydıyla Şirket meşru menfaatleri için kişisel veri işleme faaliyetinde bulunulmasının zorunlu olması
- Şirket tarafından kişisel veri işleme faaliyetinde bulunulmasının kişisel veri sahibinin ya da bir başkasının hayatı veya beden bütünlüğünün korunması için zorunlu olması ve bu durumda da kişisel veri sahibinin fiili veya hukuki geçersizlik nedeniyle rızasını açıklayamayacak durumda bulunması
- Kişisel veri sahibinin sağlığı ve cinsel hayatı dışındaki özel nitelikli kişisel veriler açısından kanunlarda öngörülmüş olması
- Kişisel veri sahibinin sağlığına ve cinsel hayatına ilişkin özel nitelikli kişisel verileri açısından ise kamu sağlığının korunması, koruyucu hekimlik, tıbbi teşhis, tedavi ve bakım hizmetlerinin yürütülmesi, sağlık hizmetleri ile finansmanının planlanması ve yönetimi amacıyla, sır saklama yükümlülüğü altında bulunan kişiler veya yetkili kurum ve kuruluşlar tarafından işlenmesidir.

4.2. Purposes of Processing Personal Data

The COMPANY processes personal data limited to the purposes and conditions included in the personal data processing conditions as stipulated in the second paragraph of the article 5 and the third paragraph of the article 6 of the PPD Act. Such purposes and conditions are the following:

- that it is clearly stipulated in laws that the COMPANY carries out operations concerning the processing of your personal data;
- that the processing of your personal data by the COMPANY is directly related to and necessary for the execution or performance of a contract;
- that the processing of your personal data is necessary so that the COMPANY may fulfil its legal obligation;
- that your personal data is to be processed by the COMPANY limited to your purpose of making public, provided that your personal data have been made public by yourself;
- that the processing of your personal data by the COMPANY is necessary for the creation, exercise or protection of the rights of the COMPANY or your or any third parties' rights;
- that it is compulsory for the COMPANY to carry out personal data processing activities for its own legitimate interests, provided that your basic rights and freedoms will not be prejudiced;
- that the COMPANY's carrying out personal data processing is necessary for the protection of the life or physical integrity of the personal data owner or any other person and that, in such a case, the personal data owner is in a condition which prevents him/her from disclosing his/her explicit consent due to physical or legal incapacity or his/her consent is not legally validated;
- that it is stipulated in laws in terms of the sensitive personal data other than the health and sexual life of the personal data owner;
- that, in terms of the sensitive personal data concerning the personal data owner's health and sexual life it is intended for the protection of public health, implementation of preventive medicine, medical diagnosis, treatment and care services and planning and management of the healthcare services and financing thereof by those individuals or competent organisations or institutions obliged to keep secrets.



PAGETEL Ltd. Şti.
İzmir- TÜRKİYE

KİŞİSEL VERİLERİN KORUNMASI VE İŞLENMESİ, KİŞİSEL VERİ SAKLAMA VE İMHA POLİTİKASI

Protection, Processing Storage and Destruction of Personal Data Policy
Kod/Code # FR-03.40

Tarih / Date :

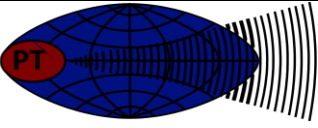
Sayfa / Page : 22 /
54

Bu kapsamda Şirket, kişisel verilerinizi aşağıdaki amaçlarla işlemektedir:

In this context, the COMPANY processes your personal data for the following purposes:

İŞLEME AMAÇLARI
Acil Durum Yönetimi Süreçlerinin Yürütülmesi
Denetim / Etik Faaliyetlerinin Yürütülmesi
İş Faaliyetlerinin Yürütülmesi / Denetimi
Yönetim Faaliyetlerinin Yürütülmesi
Finans Ve Muhasebe İşlerinin Yürütülmesi
Faaliyetlerin Mevzuata Uygun Yürütülmesi
Hukuk İşlerinin Takibi Ve Yürütülmesi
Yetkili Kişi, Kurum Ve Kuruluşlara Bilgi Verilmesi
Çalışanlar İçin İş Akdi Ve Mevzuattan Kaynaklı Yükümlülüklerin Yerine Getirilmesi
Çalışanlar İçin Yan Haklar Ve Menfaatleri Süreçlerinin Yürütülmesi
Fiziksel Mekan Güvenliğinin Temini
Ziyaretçi Kayıtlarının Oluşturulması Ve Takibi
Bilgi Güvenliği Süreçlerinin Yürütülmesi
İletişim Faaliyetlerinin Yürütülmesi
İş Süreçlerinin İyileştirilmesine Yönelik Önerilerin Alınması Ve Değerlendirilmesi
İş Sürekliliğinin Sağlanması Faaliyetlerinin Yürütülmesi
Sözleşme Süreçlerinin Yürütülmesi
İç Denetim/ Soruşturma / İstihbarat Faaliyetlerinin Yürütülmesi
Organizasyon Ve Etkinlik Yönetimi
Ücret Politikasının Yürütülmesi
Müşteri İlişkileri Yönetimi Süreçlerinin Yürütülmesi
Reklam / Kampanya / Promosyon Süreçlerinin Yürütülmesi
Risk Yönetimi Süreçlerinin Yürütülmesi
Mal / Hizmet Satın Alım Süreçlerinin Yürütülmesi
Çalışan Adayı / Stajyer / Öğrenci Seçme Ve Yerleştirme Süreçlerinin Yürütülmesi
Çalışan Adaylarının Başvuru Süreçlerinin Yürütülmesi
Çalışan Memnuniyeti Ve Bağlılığı Süreçlerinin Yürütülmesi
Eğitim Faaliyetlerinin Yürütülmesi
Erişim Yetkilerinin Yürütülmesi
Firma / Ürün / Hizmetlere Bağlılık Süreçlerinin Yürütülmesi

PURPOSES OF PROCESSING
Implementation of the Emergency Management Processes
Implementation of the Auditing / Ethical Activities
Implementation / Auditing of Business Operations
Implementation of Managerial Activities
Implementation of Financing and Accounting Operations
Implementation of the Operations in Compliance with the Legislation
Follow-up and Implementation of Legal Affairs
Provision of Authorised People, Organisations and Institutions with Information
Fulfilment of the Obligations Arising from Employment Contracts and Legislation for Employees
Implementation of the Fringe Benefits and Interests Processes for Employees
Provision of the Security of Physical Space
Creation and Tracking of Visitor Records
Implementation of Information Security Processes
Implementation of Communication Activities
Receipt and Evaluation of Suggestions for the Improvement of Business Processes
Implementation of the Activities of Ensuring Business Continuity
Implementation of Contractual Processes
Implementation of Internal Auditing / Investigation / Intelligence Operations
Organisation and Event Management
Implementation of the Waging Policy
Implementation of the Customer Relations Management Processes
Implementation of the Advertising / Campaign / Promotion Processes
Implementation of the Risk Management Processes
Implementation of the Goods / Services Purchasing Processes
Implementation of the Employee Candidate / Trainee / Student Selection and Placement Processes
Implementation of the Application Processes of Employee Candidates
Implementation of Employee Satisfaction and Commitment Processes
Implementation of Training Activities
Implementation of Access Authorisations
Implementation of the Processes of Commitment to the Company / Product / Services



PAGETEL Ltd. Şti.
İzmir- TÜRKİYE

KİŞİSEL VERİLERİN KORUNMASI VE İŞLENMESİ, KİŞİSEL VERİ SAKLAMA VE İMHA POLİTİKASI

Protection, Processing Storage and Destruction of Personal Data Policy
Kod/Code # FR-03.40

Tarih / Date :

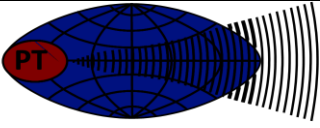
Sayfa / Page : 23 /
54

Görevlendirme Süreçlerinin Yürütülmesi
İnsan Kaynakları Süreçlerinin Planlanması
İş Sağlığı / Güvenliği Faaliyetlerinin Yürütülmesi
Lojistik Faaliyetlerinin Yürütülmesi
Mal / Hizmet Satış Sonrası Destek Hizmetlerinin Yürütülmesi
Mal / Hizmet Satış Süreçlerinin Yürütülmesi
Mal / Hizmet Üretim Ve Operasyon Süreçlerinin Yürütülmesi
Müşteri Memnuniyetine Yönelik Aktivitelerin Yürütülmesi
Pazarlama Analiz Çalışmalarının Yürütülmesi
Performans Değerlendirme Süreçlerinin Yürütülmesi
Saklama Ve Arşiv Faaliyetlerinin Yürütülmesi
Sosyal Sorumluluk Ve Sivil Toplum Aktivitelerinin Yürütülmesi
Sponsorluk Faaliyetlerinin Yürütülmesi
Stratejik Planlama Faaliyetlerinin Yürütülmesi
Talep / Şikayetlerin Takibi
Taşınır Mal Ve Kaynakların Güvenliğinin Temini
Tedarik Zinciri Yönetimi Süreçlerinin Yürütülmesi
Ürün / Hizmetlerin Pazarlama Süreçlerinin Yürütülmesi
Veri Sorumlusu Operasyonlarının Güvenliğinin Temini
Yabancı Personel Çalışma Ve Oturma İzni İşlemleri
Yatırım Süreçlerinin Yürütülmesi
Yetenek / Kariyer Gelişimi Faaliyetlerinin Yürütülmesi
Çevre Yönetim Faaliyetlerinin Yürütülmesi
Ürün/ Hizmet Kabul ve Doğrulama Süreçlerinin Yürütülmesi
İnsan Kaynakları Süreçlerinin Yürütülmesi
Personel Devam Kontrol Sisteminin Yürütülmesi
Fesih İşlemlerinin Yürütülmesi

Implementation of Assignment Processes
Planning of Human resources Processes
Implementation of Occupational Health and Safety Activities
Implementation of Logistics Operations
Implementation of Aftersales Support Services for Goods / Services
Implementation of Goods / Services Sales Processes
Implementation of Goods / Service Production and Operation Processes
Implementation of the Activities Intended for Customer Satisfaction
Implementation of Marketing Analysis Operations
Implementation of Performance Assessment Processes
Implementation of Storage and Archiving Operations
Implementation of Social Responsibility and Non-Governmental Activities
Implementation of Sponsorship Activities
Implementation of Strategic Planning Activities
Tracking of Requests / Complaints
Provision of the Security of Chattels and Resources
Implementation of the Supply Chain Management Processes
Implementation of the Marketing Processes of Products / Services
Provision of the Security of the Data Controller Operations
Foreign Personnel's Working and Residence Permit Procedures
Implementation of Investment Processes
Implementation of Ability / Career Development Activities
Implementation of Environmental Activities
Implementation of Product / Service Acceptance and Verification Processes
Implementation of Human Resources Processes
Implementation of Personnel Attendance Control System
Implementation of Termination Procedures

Bahsi geçen amaçlarla gerçekleştirilen işleme faaliyetinin, KVK Kanunu kapsamında öngörülen şartlardan herhangi birini karşılamıyor olması halinde, ilgili işleme sürecine ilişkin olarak Şirketimiz tarafından açık rızanız temin edilmektedir.

In the event that any processing activity carried out for the abovementioned purposes fails to satisfy any of the conditions stipulated by the PPD Act, then the COMPANY obtains your explicit consent for the relevant processing process.



PAGETEL Ltd. Şti.
İzmir- TÜRKİYE

KİŞİSEL VERİLERİN KORUNMASI VE İŞLENMESİ, KİŞİSEL VERİ SAKLAMA VE İMHA POLİTİKASI

Protection, Processing Storage and Destruction of Personal Data Policy
Kod/Code # FR-03.40

Tarih / Date :

Sayfa / Page : 24 /
54

4.3. Kişisel Verilerin Saklanması

4.3.1. Kişisel Verilerin Saklanma Süreleri

Şirket, ilgili kanunlarda ve mevzuatlarda öngörülmesi durumunda kişisel verileri bu mevzuatlarda belirtilen süre boyunca saklamaktadır. Şirket tarafından belirlenen saklama, imha ve periyodik imha süreleri aşağıda belirtilmiştir:

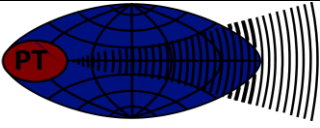
Faaliyet	Saklama Süresi	İmha Süresi
Personel İsim Listesi Oluşturulması	İş İlişkisinin Sona Ermesinden İtibaren 15 Yıl	Saklama Süresinin bitimi itibari ile ilk Periyodik İmha zamanında
Finansal Faaliyetlerin Yürütülmesi	Hukuki ilişkinin sona ermesinden itibaren 15 Yıl 14 gün 10 Yıl İş İlişkisinin Sona Ermesinden İtibaren 15 Yıl	Saklama Süresinin bitimi itibari ile ilk Periyodik İmha zamanında
Kiralama İşlemleri	Hukuki ilişkinin sona ermesinden itibaren 15 Yıl	Saklama Süresinin bitimi itibari ile ilk Periyodik İmha zamanında
Dava, İcra Takibi ve İcra Dairelerine Yapılan Ödemelerin Takibi	Hukuki ilişkinin sona ermesinden itibaren 15 Yıl	Saklama Süresinin bitimi itibari ile ilk Periyodik İmha zamanında
Dava, İcra Takibi ve İcra Daireleri İşlemlerinin Takibi	Hukuki ilişkinin sona ermesinden itibaren 15 Yıl	Saklama Süresinin bitimi itibari ile ilk Periyodik İmha zamanında
Banka ve Ödeme İşlemleri	Hukuki ilişkinin sona ermesinden itibaren 15 Yıl 3 Yıl İş İlişkisinin Sona Ermesinden İtibaren 15 Yıl	Saklama Süresinin bitimi itibari ile ilk Periyodik İmha zamanında
Maaş Ödemeleri	Hukuki ilişkinin sona ermesinden itibaren 15 Yıl 10 Yıl	Saklama Süresinin bitimi itibari ile ilk Periyodik İmha zamanında
Personel Masraf Takibi ve Ödemesi	Hukuki ilişkinin sona ermesinden itibaren 15 Yıl	Saklama Süresinin bitimi itibari ile ilk Periyodik İmha zamanında
Ödeme İşlemleri	Hukuki ilişkinin sona ermesinden itibaren 15 Yıl	Saklama Süresinin bitimi itibari ile ilk Periyodik İmha zamanında

4.3. Storage of Personal Data

4.3.1. Storage Periods of Personal Data

The COMPANY stores personal data for the period of time as indicated in the legislation in case the same is stipulated by the relevant laws and regulations. Storage, destruction and periodical destruction periods designated by the COMPANY are given below:

Activity	Storage Period	Destruction Period
Creation of Personnel's Name List	15 Years Following the Termination of Employment Relationship	At the first Periodical Destruction time as from the expiry of the storage period
Implementation of Financial Activity	15 Years Following the Termination of legal relationship 14 days 10 Years 15 Years Following the Termination of Employment Relationship	At the first Periodical Destruction time as from the expiry of the storage period
Leasing Operations	15 Years following the termination of legal relationship	At the first Periodical Destruction time as from the expiry of the storage period
Follow-up of Litigation, Execution Proceedings and Payments to Bailiff's Offices	15 Years following the termination of legal relationship	At the first Periodical Destruction time as from the expiry of the storage period
Follow-up of Litigation, Execution Proceedings and Affairs at Bailiff's Offices	15 Years following the termination of legal relationship	At the first Periodical Destruction time as from the expiry of the storage period
Bank and Payment Transactions	15 Years following the termination of legal relationship 3 Years 15 Years Following the Termination of Employment Relationship	At the first Periodical Destruction time as from the expiry of the storage period
Salary Payments	15 Years following the termination of legal relationship 10 Years	At the first Periodical Destruction time as from the expiry of the storage period
Tracking and Payment of Expense Incurred by Personnel	15 Years following the termination of legal relationship	At the first Periodical Destruction time as from the expiry of the storage period



PAGETEL Ltd. Şti.
İzmir- TÜRKİYE

KİŞİSEL VERİLERİN KORUNMASI VE İŞLENMESİ, KİŞİSEL VERİ SAKLAMA VE İMHA POLİTİKASI

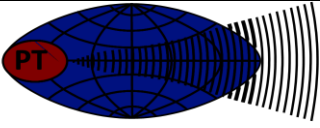
Protection, Processing Storage and Destruction of Personal Data Policy
Kod/Code # FR-03.40

Tarih / Date :

Sayfa / Page : 25 /
54

İdari İşler ve Faaliyetlerin Yürütülmesi	İş İlişkisinin Sona Ermesinden İtibaren 15 Yıl Hukuki ilişkinin sona ermesinden itibaren 15 Yıl 14 gün	Saklama Süresinin bitimi itibari ile ilk Periyodik İmha zamanında
Tesis Güvenlik Faaliyetleri	5 Yıl Belge geçerlilik süresinin sona ermesinden itibaren 5 yıl	Saklama Süresinin bitimi itibari ile ilk Periyodik İmha zamanında
İş Operasyonu	Hukuki ilişkinin sona ermesinden itibaren 15 Yıl 14 gün Revize edilmesi halinde klasörde 2 yıl, arşivde 10 yıl, serverda 50 yıl Klasörde 5 yıl, Arşivde 10 yıl, serverda 50 yıl Klasörde 5 yıl, Arşivde 10 yıl 10 Yıl İş İlişkisinin Sona Ermesinden İtibaren 15 Yıl	Saklama Süresinin bitimi itibari ile ilk Periyodik İmha zamanında
Yönetimin Gözden Geçirilmesi Süreci	Hukuki ilişkinin sona ermesinden itibaren 15 Yıl 5 yıl klasörde, 10 yıl arşivde, 50 yıl serverda 50 Yıl Revize edilmesi halinde klasörde 2 yıl, arşivde 10 yıl, serverda 50 yıl	Saklama Süresinin bitimi itibari ile ilk Periyodik İmha zamanında
Ticari Faaliyetin Yürütülmesi	Hukuki ilişkinin sona ermesinden itibaren 15 Yıl	Saklama Süresinin bitimi itibari ile ilk Periyodik İmha zamanında
Sigorta Süreci	Hukuki ilişkinin sona ermesinden itibaren 15 Yıl	Saklama Süresinin bitimi itibari ile ilk Periyodik İmha zamanında
Denetim Faaliyetleri	Hukuki ilişkinin sona ermesinden itibaren 15 Yıl Klasörde 15 yıl, serverda 50 yıl 50 Yıl EYS klasöründe 5 yıl Arşivde 10 yıl Serverda 50 yıl Revize edilmesi halinde klasörde 2 yıl, arşivde 10 yıl, serverda 50 yıl	Saklama Süresinin bitimi itibari ile ilk Periyodik İmha zamanında
Sözleşme Süreçlerinin Takibi	Hukuki ilişkinin sona ermesinden itibaren 15 Yıl	Saklama Süresinin bitimi itibari ile ilk Periyodik İmha zamanında
Gelen Evrak Kayıt	Hukuki ilişkinin sona ermesinden itibaren 15 Yıl	Saklama Süresinin bitimi itibari ile ilk Periyodik İmha zamanında

Payment Transactions	15 Years following the termination of legal relationship	At the first Periodical Destruction time as from the expiry of the storage period
Implementation of Legal Procedures	15 Years Following the Termination of Employment Relationship 15 Years following the termination of legal relationship 14 days	At the first Periodical Destruction time as from the expiry of the storage period
Implementation of Administrative Affairs and Activities	15 Years Following the Termination of Employment Relationship 15 Years following the termination of legal relationship 14 days	At the first Periodical Destruction time as from the expiry of the storage period
Plant Security Activities	5 Years 5 Years following the expiry of the validity of certificate	At the first Periodical Destruction time as from the expiry of the storage period
Business Operations	15 Years following the termination of legal relationship 14 days In case of revision, 2 years in folder; 10 years in archive and 50 years in server; 5 years in folder, 10 years in archive, 50 years in server 5 years in folder, 10 years in archive 10 Years 15 Years Following the Termination of Employment Relationship	At the first Periodical Destruction time as from the expiry of the storage period
Management's Review Process	15 Years following the termination of legal relationship 5 years in folder; 10 years in archive and 50 years in server 50 Yıl In case of revision, 2 years in folder; 10 years in archive and 50 years in server	At the first Periodical Destruction time as from the expiry of the storage period
Implementation of Commercial Activities	15 Years following the termination of legal relationship	At the first Periodical Destruction time as from the expiry of the storage period
Insurance Process	15 Years following the termination of legal relationship	At the first Periodical Destruction time as from the expiry of the storage period
Auditing Activities	15 Years following the termination of legal relationship 15 years in folder; 50 years in server 50 Years 5 Years in EYS folder, 10 years in archive and 50 years in server In case of revision, 2 years in folder; 10 years in archive and 50 years in server	At the first Periodical Destruction time as from the expiry of the storage period



PAGETEL Ltd. Şti.
İzmir- TÜRKİYE

KİŞİSEL VERİLERİN KORUNMASI VE İŞLENMESİ, KİŞİSEL VERİ SAKLAMA VE İMHA POLİTİKASI

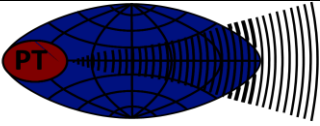
Protection, Processing Storage and Destruction of Personal Data Policy
Kod/Code # FR-03.40

Tarih / Date :

Sayfa / Page : 26 /
54

Muhasebe departmanına gelen evrakların, yazışmaların takibi ve cevaplanması	Hukuki ilişkinin sona ermesinden itibaren 15 Yıl	Saklama Süresinin bitimi itibari ile ilk Periyodik İmha zamanında
Kasa Operasyon Süreci	Hukuki ilişkinin sona ermesinden itibaren 15 Yıl	Saklama Süresinin bitimi itibari ile ilk Periyodik İmha zamanında
Taşınır ve Taşınmaz Yönetimi	Hukuki ilişkinin sona ermesinden itibaren 15 Yıl	Saklama Süresinin bitimi itibari ile ilk Periyodik İmha zamanında
Sayım Süreci	Hukuki ilişkinin sona ermesinden itibaren 15 Yıl 10 Yıl	Saklama Süresinin bitimi itibari ile ilk Periyodik İmha zamanında
Bireysel Emeklilik Sistemi (BES) Süreci	Hukuki ilişkinin sona ermesinden itibaren 15 Yıl İş İlişkinin Sona Ermesinden İtibaren 15 Yıl	Saklama Süresinin bitimi itibari ile ilk Periyodik İmha zamanında
Bordro ve Maaş Dosyasının Hazırlanması	Hukuki ilişkinin sona ermesinden itibaren 15 Yıl İş İlişkinin Sona Ermesinden İtibaren 15 Yıl	Saklama Süresinin bitimi itibari ile ilk Periyodik İmha zamanında
Dava ve İcra Takip Süreci	Hukuki ilişkinin sona ermesinden itibaren 15 Yıl İş İlişkinin Sona Ermesinden İtibaren 15 Yıl	Saklama Süresinin bitimi itibari ile ilk Periyodik İmha zamanında
Resmi Kurum ve Kuruluş İşlemleri	Hukuki ilişkinin sona ermesinden itibaren 15 Yıl	Saklama Süresinin bitimi itibari ile ilk Periyodik İmha zamanında
SGK-Tahakkuk İşlemleri	Hukuki ilişkinin sona ermesinden itibaren 15 Yıl İş İlişkinin Sona Ermesinden İtibaren 15 Yıl	Saklama Süresinin bitimi itibari ile ilk Periyodik İmha zamanında
Muhasebe Kaydı Yapılması	Hukuki ilişkinin sona ermesinden itibaren 15 Yıl 10 Yıl	Saklama Süresinin bitimi itibari ile ilk Periyodik İmha zamanında
İnsan Kaynakları Faaliyetlerinin Yürütülmesi	Hukuki ilişkinin sona ermesinden itibaren 15 Yıl 14 gün 10 Yıl Revize edilmesi halinde klasörde 2 yıl, arşivde 10 yıl, serverda 50 yıl İş İlişkinin Sona Ermesinden İtibaren 15 Yıl 5 Yıl	Saklama Süresinin bitimi itibari ile ilk Periyodik İmha zamanında Silinme Talebi sonrası 30 gün cevap verme süresi içinde

Follow-up of Contractual Processes	15 Years following the termination of legal relationship	At the first Periodical Destruction time as from the expiry of the storage period
Incoming Document Entry	15 Years following the termination of legal relationship	At the first Periodical Destruction time as from the expiry of the storage period
Following up and replying documents and correspondence arriving at the accounting department	15 Years following the termination of legal relationship	At the first Periodical Destruction time as from the expiry of the storage period
Cash Operations Process	15 Years following the termination of legal relationship	At the first Periodical Destruction time as from the expiry of the storage period
Chattel and Property Management	15 Years following the termination of legal relationship	At the first Periodical Destruction time as from the expiry of the storage period
Counting Process	15 Years following the termination of legal relationship 10 Years	At the first Periodical Destruction time as from the expiry of the storage period
Individual Pension System (BES) Process	15 Years following the termination of legal relationship 15 Years Following the Termination of Employment Relationship	At the first Periodical Destruction time as from the expiry of the storage period
Preparation of Payroll and Salary File	15 Years following the termination of legal relationship 15 Years Following the Termination of Employment Relationship	At the first Periodical Destruction time as from the expiry of the storage period
Litigation and Execution Proceedings Process	15 Years following the termination of legal relationship 15 Years Following the Termination of Employment Relationship	At the first Periodical Destruction time as from the expiry of the storage period



PAGETEL Ltd. Şti.
İzmir- TÜRKİYE

KİŞİSEL VERİLERİN KORUNMASI VE İŞLENMESİ, KİŞİSEL VERİ SAKLAMA VE İMHA POLİTİKASI

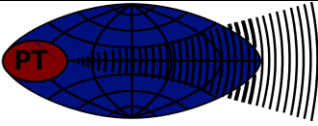
Protection, Processing Storage and Destruction of Personal Data Policy
Kod/Code # FR-03.40

Tarih / Date :

Sayfa / Page : 27 /
54

GD Anti-Bribery politikasını şirkete adapte etmek ve Anti-Bribery Coordinator'e destek olmak	Hukuki ilişkinin sona ermesinden itibaren 15 Yıl
Dış Kaynaklı Denetim Süreci	Hukuki ilişkinin sona ermesinden itibaren 15 Yıl 14 gün
Ortaklıklarla yapılan yazışmalar	Hukuki ilişkinin sona ermesinden itibaren 15 Yıl
Müşteri İlişkilerinin Yönetilmesi Süreci	Hukuki ilişkinin sona ermesinden itibaren 15 Yıl Proje teslimatından itibaren 20 yıl Revize edilmesi halinde klasörde 2 yıl, arşivde 10 yıl, serverda 50 yıl
BA/BS Beyanname Süreci	Hukuki ilişkinin sona ermesinden itibaren 15 Yıl
Bilgi Teknolojileri Sistemleri Süreçleri	10 Yıl 3 Yıl 14 gün 3 Ay Revize edilmesi halinde klasörde 2 yıl, arşivde 10 yıl, serverda 50 yıl İş İlişkisinin Sona Ermesinden İtibaren 15 Yıl
Beyanname Süreci	Hukuki ilişkinin sona ermesinden itibaren 15 Yıl İş İlişkisinin Sona Ermesinden İtibaren 15 Yıl
Satın Alma ve Tedarik Faaliyetleri	Hukuki ilişkinin sona ermesinden itibaren 15 Yıl 10 Yıl 50 Yıl Klasörde 5 yıl, Arşivde 10 yıl, serverda 50 yıl Klasörde 5 yıl, Arşivde 10 yıl Revize edilmesi halinde klasörde 2 yıl, arşivde 10 yıl, serverda 50 yıl Proje süresince Satın Alma Biriminde klasörde, Arşiv odasında 10 yıl Hukuki ilişkinin sona ermesinden sonra 10 yıl
Bilgi İşlem Operasyonlarının Yürütülmesi	10 Yıl 6 Ay
Müşteri İletişiminin Sağlanması	Hukuki ilişkinin sona ermesinden itibaren 15 Yıl
Eğitim Faaliyetleri	14 gün İş İlişkisinin Sona Ermesinden İtibaren 15 Yıl

Procedures before Public Organisations and Authorities	15 Years following the termination of legal relationship	At the first Periodical Destruction time as from the expiry of the storage period
SSO-Accrual Transactions	15 Years following the termination of legal relationship 15 Years Following the Termination of Employment Relationship	At the first Periodical Destruction time as from the expiry of the storage period
Carrying out Accounting Entries	15 Years following the termination of legal relationship 10 Years	At the first Periodical Destruction time as from the expiry of the storage period
Implementation of Human Resources Activities	15 Years following the termination of legal relationship 14 days 10 Years In case of revision, 2 years in folder; 10 years in archive and 50 years in server 15 Years Following the Termination of Employment Relationship 5 Years	At the first Periodical Destruction time as from the expiry of the storage period Within replying period of 30 days following the request for deletion
To adapt GD Anti-Bribery policies to the Company and support the Anti-Bribery Coordinator	15 Years following the termination of legal relationship	At the first Periodical Destruction time as from the expiry of the storage period
External Auditing Process	15 Years following the termination of legal relationship 14 days	At the first Periodical Destruction time as from the expiry of the storage period
Correspondence with Subsidiaries	15 Years following the termination of legal relationship	At the first Periodical Destruction time as from the expiry of the storage period
Customer Relations Management Process	15 Years following the termination of legal relationship 20 years following the project delivery In case of revision, 2 years in folder; 10 years in archive and 50 years in server	At the first Periodical Destruction time as from the expiry of the storage period
Product Verification Process	10 Years in relevant project folder and 10 years in archive afterwards and 50 years in server	At the first Periodical Destruction time as from the expiry of the storage period
On-the-Job Training Planning	15 Years Following the Termination of Employment Relationship	At the first Periodical Destruction time as from the expiry of the storage period
Implementation of EYS Document Management Activities	In case of revision, 2 years in folder and 10 years in archive	At the first Periodical Destruction time as from the expiry of the storage period



PAGETEL Ltd. Şti.
İzmir- TÜRKİYE

KİŞİSEL VERİLERİN KORUNMASI VE İŞLENMESİ, KİŞİSEL VERİ SAKLAMA VE İMHA POLİTİKASI

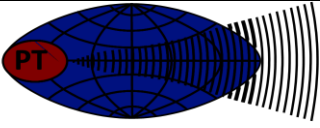
Protection, Processing Storage and Destruction of Personal Data Policy
Kod/Code # FR-03.40

Tarih / Date :

Sayfa / Page : 28 /
54

Entegre Sistem Yönetimi	14 gün Revize edilmesi halinde klasörde 2 yıl, arşivde 10 yıl, serverda 50 yıl 50 Yıl Hukuki ilişkinin sona ermesinden sonra 10 yıl 5 yıl klasörde, 10 yıl arşivde, 50 yıl serverda 2 yıl klasörde 10 yıl arşivde	Saklama Süresinin bitimi itibari ile ilk Periyodik İmha zamanında
İzin İşlemlerinin Yürütülmesi	14 gün 10 Yıl İş İlişkisinin Sona Ermesinden İtibaren 15 Yıl	Saklama Süresinin bitimi itibari ile ilk Periyodik İmha zamanında
Kalite Kontrol Süreci	14 gün 10 Yıl Klasörde 5 yıl, Arşivde 10 yıl, serverda 50 yıl Klasörde 5 yıl, Arşivde 10 yıl Revize edilmesi halinde klasörde 2 yıl, arşivde 10 yıl, serverda 50 yıl Revize edilmesi halinde klasörde 2 yıl, arşivde 5 yıl, serverda 50 yıl 10 yıl ilgili proje klasöründe, sonrasında 10 yıl arşivde, 50 yıl serverda	Saklama Süresinin bitimi itibari ile ilk Periyodik İmha zamanında
Depolama ve Sevkiyat Süreci	14 gün Revize edilmesi halinde klasörde 2 yıl, arşivde 10 yıl, serverda 50 yıl	Saklama Süresinin bitimi itibari ile ilk Periyodik İmha zamanında
İnsan Kaynakları Süreci	14 gün 10 Yıl Revize edilmesi halinde klasörde 2 yıl, arşivde 10 yıl, serverda 50 yıl	Saklama Süresinin bitimi itibari ile ilk Periyodik İmha zamanında
Nakit Akış Planlama ve Raporlama	10 Yıl	Saklama Süresinin bitimi itibari ile ilk Periyodik İmha zamanında
Sevkiyat işlerinin takibi ve teslimi	10 Yıl Hukuki ilişkinin sona ermesinden sonra 10 yıl	Saklama Süresinin bitimi itibari ile ilk Periyodik İmha zamanında
Kartlı Sistem Kontrolü (PDKS)	3 Ay İş İlişkisinin Sona Ermesinden İtibaren 15 Yıl 2 Yıl	Silinme/İmha Talebi ile hemen silinir ve yok edilir Saklama Süresinin bitimi itibari ile ilk Periyodik İmha zamanında Silinme Talebi sonrası 30 gün cevap verme süresi içinde

BA/BS Declaration Process	15 Years following the termination of legal relationship	At the first Periodical Destruction time as from the expiry of the storage period
Information Technologies System Process	10 Years 3 Years 14 days 3 Months In case of revision, 2 years in folder; 10 years in archive and 50 years in server 15 Years Following the Termination of Employment Relationship	At the first Periodical Destruction time as from the expiry of the storage period Immediately deleted and destroyed upon Deletion/ Destruction Request
Declaration Process	15 Years following the termination of legal relationship 15 Years Following the Termination of Employment Relationship	At the first Periodical Destruction time as from the expiry of the storage period
Purchasing and Procurement Operations	15 Years following the termination of legal relationship 10 Years 50 Years 5 years in folder, 10 years in archive and 50 years in server 5 years in folder, 10 years in archive In case of revision, 2 years in folder; 10 years in archive and 50 years in server 10 years in folder and archive room at the Purchasing Department during the Project 10 years following the termination of legal relationship	At the first Periodical Destruction time as from the expiry of the storage period
Implementation of Data Processing Operations	10 Years 6 Months	Immediately deleted and destroyed upon Deletion/ Destruction Request
Provision of Communication with Customer	15 Years following the termination of legal relationship	At the first Periodical Destruction time as from the expiry of the storage period
Training Activities	14 days 15 Years Following the Termination of Employment Relationship	At the first Periodical Destruction time as from the expiry of the storage period
Implementation of Permit Procedures	14 days 10 Years 15 Years Following the Termination of Employment Relationship	At the first Periodical Destruction time as from the expiry of the storage period
Creation of Personal File of an Employee	15 Years Following the Termination of Employment Relationship	At the first Periodical Destruction time as from the expiry of the storage period
Recruitment Process	15 Years Following the Termination of Employment Relationship 5 Years	At the first Periodical Destruction time as from the expiry of the storage period Within replying period of 30 days following the request for deletion



PAGETEL Ltd. Şti.
İzmir- TÜRKİYE

KİŞİSEL VERİLERİN KORUNMASI VE İŞLENMESİ, KİŞİSEL VERİ SAKLAMA VE İMHA POLİTİKASI

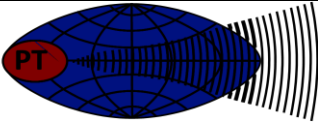
Protection, Processing Storage and Destruction of Personal Data Policy
Kod/Code # FR-03.40

Tarih / Date :

Sayfa / Page : 29 /
54

Web sayfası yönetimi	3 Ay 3 Yıl	Silinme/İmha Talebi ile hemen silinir ve yok edilir Saklama Süresinin bitimi itibari ile ilk Periyodik İmha zamanında
Yüz Okutma Sistemi Kontrolü (PDKS)	3 Ay İş İlişkisinin Sona Ermesinden İtibaren 15 Yıl 2 Yıl	Silinme/İmha Talebi ile hemen silinir ve yok edilir Saklama Süresinin bitimi itibari ile ilk Periyodik İmha zamanında Silinme Talebi sonrası 30 gün cevap verme süresi içinde
İş Sağlığı ve Güvenliği Faaliyetlerinin Yürütülmesi	Revize edilmesi halinde klasörde 2 yıl, arşivde 10 yıl, serverda 50 yıl İş İlişkisinin Sona Ermesinden İtibaren 15 Yıl İş İlişkisinin Sona Ermesinden İtibaren 15 Yıl 1 yıl depo bölümünde klasörde 10 yıl arşiv odasında Pandemi bitimi itibari ile 6 ay	Saklama Süresinin bitimi itibari ile ilk Periyodik İmha zamanında
Çevre Yönetim Faaliyetlerinin Yürütülmesi	5 yıl klasörde, 10 yıl arşivde, 50 yıl serverda Revize edilmesi halinde klasörde 2 yıl, arşivde 10 yıl, serverda 50 yıl Klasörde 15 yıl, serverda 50 yıl	Saklama Süresinin bitimi itibari ile ilk Periyodik İmha zamanında
Ürün/ Hizmet Faaliyetlerinin Yürütülmesi Süreci	Revize edilmesi halinde klasörde 2 yıl, arşivde 10 yıl, serverda 50 yıl Klasörde 5 yıl, Arşivde 10 yıl, serverda 50 yıl Hukuki ilişkinin sona ermesinden sonra 10 yıl	Saklama Süresinin bitimi itibari ile ilk Periyodik İmha zamanında

Integrated System Management	14 days In case of revision, 2 years in folder; 10 years in archive and 50 years in server 50 Years 10 Years following the termination of legal relationship 5 years in folder; 10 years in archive and 50 years in server 2 years in folder, 10 years in archive	At the first Periodical Destruction time as from the expiry of the storage period
Quality Control Process	14 days 10 Years 5 years in folder, 10 years in archive and 50 years in server 5 years in folder, 10 years in archive In case of revision, 2 years in folder; 10 years in archive and 50 years in server In case of revision, 2 years in folder, 5 years in archive and 50 years in server 10 Years in relevant project folder, 10 years in archive afterwards and 50 years in server	At the first Periodical Destruction time as from the expiry of the storage period
Storage and Shipment Process	14 days In case of revision, 2 years in folder; 10 years in archive and 50 years in server	At the first Periodical Destruction time as from the expiry of the storage period
Human Resources Process	14 days 10 Years In case of revision, 2 years in folder; 10 years in archive and 50 years in server	At the first Periodical Destruction time as from the expiry of the storage period
Cash Flow Planning and Reporting	10 Years	At the first Periodical Destruction time as from the expiry of the storage period
Tracking and delivery of shipment operations	10 Years 10 Years following the termination of legal relationship	At the first Periodical Destruction time as from the expiry of the storage period
Card System Control (PDKS)	3 Months 15 Years Following the Termination of Employment Relationship 2 Years	Immediately deleted/destroyed upon Deletion/Destruction Request At the first Periodical Destruction time as from the expiry of the storage period Within replying period of 30 days following the request for deletion
Termination Procedures	15 Years Following the Termination of Employment Relationship	At the first Periodical Destruction time as from the expiry of the storage period



PAGETEL Ltd. Şti.
İzmir- TÜRKİYE

KİŞİSEL VERİLERİN KORUNMASI VE İŞLENMESİ, KİŞİSEL VERİ SAKLAMA VE İMHA POLİTİKASI

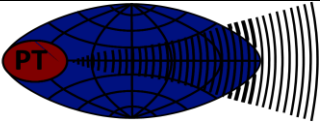
Protection, Processing Storage and Destruction of Personal Data Policy
Kod/Code # FR-03.40

Tarih / Date :

Sayfa / Page : 30 /
54

Bakım Onarım Süreci	Revize edilmesi halinde klasörde 2 yıl, arşivde 10 yıl, serverda 50 yıl	Saklama Süresinin bitimi itibari ile ilk Periyodik İmha zamanında
İşkur İşlemleri	3 Yıl İş ilişkisinin Sona Ermesinden İtibaren 15 Yıl	Saklama Süresinin bitimi itibari ile ilk Periyodik İmha zamanında
Müşteri Geri Bildirimi Alınması	Proje teslimatından itibaren 20 yıl	Saklama Süresinin bitimi itibari ile ilk Periyodik İmha zamanında
Satış Sonrası Servis Faaliyetlerinin Yürütülmesi	Proje teslimatından itibaren 20 yıl 10 yıl klasörde, 10 yıl arşivde	Saklama Süresinin bitimi itibari ile ilk Periyodik İmha zamanında
İşyeri içinde ve dışında Görüntü Kayıt Sistemi	İş ilişkisinin Sona Ermesinden İtibaren 15 Yıl	Saklama Süresinin bitimi itibari ile ilk Periyodik İmha zamanında
Personel Devam Kontrol Listesi	İş ilişkisinin Sona Ermesinden İtibaren 15 Yıl	Saklama Süresinin bitimi itibari ile ilk Periyodik İmha zamanında Silinme Talebi sonrası 30 gün cevap verme süresi içinde
Sistem odası güvenliğinin sağlanması	İş ilişkisinin Sona Ermesinden İtibaren 15 Yıl	Saklama Süresinin bitimi itibari ile ilk Periyodik İmha zamanında
Entegre Sistem Doküman Yönetim Süreci	İş ilişkisinin Sona Ermesinden İtibaren 15 Yıl Revize edilmesi halinde 2 yıl klasörde 10 yıl arşivde	Saklama Süresinin bitimi itibari ile ilk Periyodik İmha zamanında
Parmak Okutma Sistemi Kontrolü (PDKS)	İş ilişkisinin Sona Ermesinden İtibaren 15 Yıl 2 Yıl	Saklama Süresinin bitimi itibari ile ilk Periyodik İmha zamanında Silinme Talebi sonrası 30 gün cevap verme süresi içinde
Posta - Kargo Gönderimleri	10 Yıl	Saklama Süresinin bitimi itibari ile ilk Periyodik İmha zamanında
Mal Kabul Süreci	Hukuki ilişkinin sona ermesinden sonra 10 yıl	Saklama Süresinin bitimi itibari ile ilk Periyodik İmha zamanında

Web Page Management	3 Months 3 Years	Immediately deleted/destroyed upon Deletion/Destruction Request At the first Periodical Destruction time as from the expiry of the storage period
Face Scanning System Control (PDKS)	3 Months 15 Years Following the Termination of Employment Relationship 2 Years	Immediately deleted/destroyed upon Deletion/Destruction Request At the first Periodical Destruction time as from the expiry of the storage period Within replying period of 30 days following the request for deletion
Implementation of Occupational Health and Safety Activities	In case of revision, 2 years in folder; 10 years in archive and 50 years in server 15 Years Following the Termination of Employment Relationship 15 Years Following the Termination of Employment Relationship 1 year in folder at the warehouse department and 10 years in archive room 6 months in archive room as of the termination of pandemic	At the first Periodical Destruction time as from the expiry of the storage period
Implementation of Environmental Management Activities	5 years in folder; 10 years in archive and 50 years in server In case of revision, 2 years in folder; 10 years in archive and 50 years in server 15 years in folder; 50 years in server	At the first Periodical Destruction time as from the expiry of the storage period
Implementation of Product/Service Activities Process	In case of revision, 2 years in folder; 10 years in archive and 50 years in server 5 years in folder, 10 years in archive and 50 years in server 10 Years following the termination of legal relationship	At the first Periodical Destruction time as from the expiry of the storage period
Maintenance and Repair Process	In case of revision, 2 years in folder; 10 years in archive and 50 years in server	At the first Periodical Destruction time as from the expiry of the storage period
Employment Agency Procedures	3 Years 15 Years Following the Termination of Employment Relationship	At the first Periodical Destruction time as from the expiry of the storage period
Receipt of Customer Feedback	20 years following the project delivery	At the first Periodical Destruction time as from the expiry of the storage period
Implementation of Aftersales Service Activities	20 years following the project delivery 10 Years in folder and 10 Years in archive	At the first Periodical Destruction time as from the expiry of the storage period



PAGETEL Ltd. Şti.
İzmir- TÜRKİYE

KİŞİSEL VERİLERİN KORUNMASI VE İŞLENMESİ, KİŞİSEL VERİ SAKLAMA VE İMHA POLİTİKASI

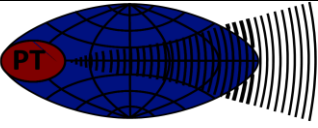
Protection, Processing Storage and Destruction of Personal Data Policy
Kod/Code # FR-03.40

Tarih / Date :

Sayfa / Page : 31 /
54

Araç Takip Sistemi Süreçleri	3 Ay	Saklama Süresinin bitimi itibari ile ilk Periyodik İmha zamanında
Çalışan İstihdamı	İş İlişkisinin Sona Ermesinden İtibaren 15 Yıl 5 Yıl	Saklama Süresinin bitimi itibari ile ilk Periyodik İmha zamanında Silinme Talebi sonrası 30 gün cevap verme süresi içinde
Çalışanın Özlük Dosyasının Oluşturulması	İş İlişkisinin Sona Ermesinden İtibaren 15 Yıl	Saklama Süresinin bitimi itibari ile ilk Periyodik İmha zamanında
İşe Giriş Süreci	İş İlişkisinin Sona Ermesinden İtibaren 15 Yıl 5 Yıl	Saklama Süresinin bitimi itibari ile ilk Periyodik İmha zamanında Silinme Talebi sonrası 30 gün cevap verme süresi içinde
İş Sağlığı ve Güvenliği Eğitimi ve Faaliyetlerinin Yürütülmesi	İş İlişkisinin Sona Ermesinden İtibaren 15 Yıl	Saklama Süresinin bitimi itibari ile ilk Periyodik İmha zamanında
Ürün Doğrulama Süreci	10 yıl ilgili proje klasöründe, sonrasında 10 yıl arşivde, 50 yıl serverda	Saklama Süresinin bitimi itibari ile ilk Periyodik İmha zamanında
Hizmetçi Eğitim Planlaması	İş İlişkisinin Sona Ermesinden İtibaren 15 Yıl	Saklama Süresinin bitimi itibari ile ilk Periyodik İmha zamanında
EYS Doküman Yönetimi Faaliyetlerinin Yürütülmesi	Revize edilmesi halinde 2 yıl klasörde 10 yıl arşivde	Saklama Süresinin bitimi itibari ile ilk Periyodik İmha zamanında
Borç Talep İşlemlerinin Yürütülmesi	İş İlişkisinin Sona Ermesinden İtibaren 15 Yıl	Saklama Süresinin bitimi itibari ile ilk Periyodik İmha zamanında
Fesih İşlemleri	İş İlişkisinin Sona Ermesinden İtibaren 15 Yıl	Saklama Süresinin bitimi itibari ile ilk Periyodik İmha zamanında
Teşviklerin Kontrolü	İş İlişkisinin Sona Ermesinden İtibaren 15 Yıl	Saklama Süresinin bitimi itibari ile ilk Periyodik İmha zamanında
İşe Başvuru Faaliyetlerinin Yürütülmesi	5 Yıl	Saklama Süresinin bitimi itibari ile ilk Periyodik İmha zamanında Silinme Talebi sonrası 30 gün cevap verme süresi içinde
Entegre Sistem Planlaması	Revize edilmesi halinde klasörde 2 yıl, arşivde 10 yıl, serverda 50 yıl	Saklama Süresinin bitimi itibari ile ilk Periyodik İmha zamanında

Image Recoding System within the workplace and without	15 Years Following the Termination of Employment Relationship	At the first Periodical Destruction time as from the expiry of the storage period
Personnel Attendance Checklist	15 Years Following the Termination of Employment Relationship	At the first Periodical Destruction time as from the expiry of the storage period Within replying period of 30 days following the request for deletion
Provision of the security of the system room	15 Years Following the Termination of Employment Relationship	At the first Periodical Destruction time as from the expiry of the storage period
Integrated System Document Management Process	15 Years Following the Termination of Employment Relationship In case of revision, 2 years in folder and 10 years in archive	At the first Periodical Destruction time as from the expiry of the storage period
Finger Scanning System Control (PDKS)	15 Years Following the Termination of Employment Relationship 2 Years	At the first Periodical Destruction time as from the expiry of the storage period Within replying period of 30 days following the request for deletion
Mail - Cargo Consignments	10 Years	At the first Periodical Destruction time as from the expiry of the storage period
Goods Acceptance Process	10 Years following the termination of legal relationship	At the first Periodical Destruction time as from the expiry of the storage period
Vehicle Tracking System Processes	3 Months	At the first Periodical Destruction time as from the expiry of the storage period
Employment of Employees	15 Years Following the Termination of Employment Relationship 5 Years	At the first Periodical Destruction time as from the expiry of the storage period Within replying period of 30 days following the request for deletion
Implementation of Occupational Health and Safety Training and Activities	15 Years Following the Termination of Employment Relationship	At the first Periodical Destruction time as from the expiry of the storage period
Implementation of Debt Claim Procedures	15 Years Following the Termination of Employment Relationship	At the first Periodical Destruction time as from the expiry of the storage period
Control of Incentives	15 Years Following the Termination of Employment Relationship	At the first Periodical Destruction time as from the expiry of the storage period
Implementation of Job Application Activities	5 Years	At the first Periodical Destruction time as from the expiry of the storage period Within replying period of 30 days following the request for deletion
Integrated System Planning	In case of revision, 2 years in folder; 10 years in archive and 50 years in server	At the first Periodical Destruction time as from the expiry of the storage period



PAGETEL Ltd. Şti.
İzmir- TÜRKİYE

KİŞİSEL VERİLERİN KORUNMASI VE İŞLENMESİ, KİŞİSEL VERİ SAKLAMA VE İMHA POLİTİKASI

Protection, Processing Storage and Destruction of Personal Data Policy
Kod/Code # FR-03.40

Tarih / Date :

Sayfa / Page : 32 /
54

Bu kapsamda kişisel veriler Kanunlar çerçevesinde öngörülen asgari saklama süreleri kadar saklanmaktadır:

Kişisel verilerin ne kadar süre boyunca saklanması gerektiğine ilişkin mevzuatta bir süre düzenlenmemişse, Kişisel Veriler Şirketin o veriyi işlerken yürütülen faaliyet ile bağlı olarak Şirketin uygulamaları ve ticari yaşamının teamülleri uyarınca işlenmesini gerektiren süre kadar işlenmekte daha sonra silinmekte, yok edilmekte veya anonim hale getirilmektedir. Bu konu ile ilgili ayrıntılı bilgiye bu Politika'nın 9. Bölümünde yer verilmiştir.

Kişisel verilerin işleme amacı sona ermiş; ilgili mevzuat ve Şirketin belirlediği saklama sürelerinin de sonuna gelmişse; kişisel veriler yalnızca olası hukuki uyumsuzluklarda delil teşkil etmesi veya kişisel veriye bağlı ilgili hakların sürülebilmesi veya savunmanın tesis edilmesi amacıyla saklanabilmektedir. Buradaki sürelerin tesisinde bahsi geçen hakkın ileri sürülebilmesine yönelik zaman aşımı süreleri ile zaman aşımı sürelerinin geçmesine rağmen daha önce aynı konularda Şirkete yöneltilen taleplerdeki örnekler esas alınarak saklama süreleri belirlenmektedir. Bu durumda saklanan kişisel verilere herhangi bir başka amaçla erişilmemekte ve ancak ilgili hukuki uyumsuzlukta kullanılması gerektiği zaman ilgili kişisel verilere erişim sağlanmaktadır. Burada da bahsi geçen süre sona erdikten sonra kişisel veriler silinmekte, yok edilmekte veya anonim hale getirilmektedir.

4.3.2. Sorumluluk ve Görev Dağılımları

Şirket'in tüm birimleri ve çalışanları, sorumlu birimlerce Politika kapsamında alınmakta olan teknik ve idari tedbirlerin gereği gibi uygulanması, birim çalışanlarının eğitimi ve farkındalığının artırılması, izlenmesi ve sürekli denetimi ile kişisel verilerin hukuka aykırı olarak işlenmesinin önlenmesi, kişisel verilere hukuka aykırı olarak erişilmesinin önlenmesi ve kişisel verilerin hukuka uygun saklanması sağlanması amacıyla kişisel veri işlenen tüm ortamlarda veri güvenliğini sağlamaya yönelik teknik ve idari tedbirlerin alınması konularında sorumlu birimlere aktif olarak destek verir.

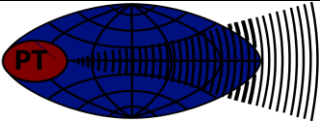
In this context, personal data are stored for the minimum storage periods as stipulated by laws:

In case any period of time is designated about how long personal data should be stored, Personal Data are processed for the period which requires such data to be stored as per the applications of the COMPANY and the practices of business life depending on the activity carried out in processing such data by the COMPANY and then deleted, destroyed or anonymized. Detailed information on the matter is provided in Section 9 of this Policy.

In case the processing purpose of personal data has ceased to exist and if the storage periods as determined by the relevant legislation and the COMPANY have expired, then may only be stored in order to constitute evidence in any possible legal controversies or to claim any relevant right dependent on personal data or to constitute the defence. In determining the periods here are considered the prescription periods for claiming the said right as well as any examples in the requests previously addressed to the COMPANY on the same issues despite the expiry of prescription, thus determining the storage periods. In this case, the personal data so stored may not be accessed for any other purposes and relevant personal data may only be accessed whenever they have to be used in any legal disputes. Personal data are deleted, destroyed or anonymized once the period mentioned here has expired.

4.3.2. Responsibilities and Task Divisions

All departments and employees of the COMPANY dynamically provide the responsible departments with support in the proper implementation of any technical and administrative taken under this Policy for providing data security in all media by which personal data are processed for the training and enhancement of awareness, monitoring and continuous control of the department employees, prevention of illegal processing of personal data, prevention of illegal access to personal data, provision of legal storage of personal data by the responsible departments.



PAGETEL Ltd. Şti.
İzmir- TÜRKİYE

KİŞİSEL VERİLERİN KORUNMASI VE İŞLENMESİ, KİŞİSEL VERİ SAKLAMA VE İMHA POLİTİKASI

Protection, Processing Storage and Destruction of Personal Data Policy
Kod/Code # FR-03.40

Tarih / Date :

Sayfa / Page : 33 /
54

4.3.3. Kayıt Ortamları

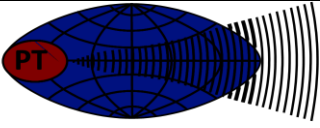
Veri sahiplerine ait kişisel veriler, Şirket tarafından aşağıdaki tabloda listelenen ortamlarda başta KVKK hükümleri olmak üzere ilgili mevzuata uygun olarak güvenli bir şekilde saklanmaktadır:

Saklama Ortamları
Kilitli Arşiv Dolabı
Server
Yurtiçi e-posta Sunucusu
Bilgisayar
Defter
Kilitli Dolap
Kontrollü Bölgede Çift Kilitli Dolap
Excel Programı
İşletme Sunucusu
Yazılım Programı
Yurtdışı Sunucu
EYS Klasörü
Arşiv Odası
Satın Alma Biriminde klasörde
Kimya mühendisi sorumluluğunda klasörde
Satın Alma biriminde klasörde
Kalite biriminde klasörde
Kalite Klasörü
Online Yedekleme Lokasyonu
Online Yedekleme Lokasyonu - 2
Satın alma Biriminde Klasörde
Depo Biriminde Klasörde
Satın Alma Biriminde Klasörde
Hard Disk
Şifreli Dosya
Arşiv Dolabı
Proje Klasörü

4.3.3. Recording Media

Personal data belonging to data owners are securely stored in the media as listed in the table below in compliance with the relevant regulations including but not limited to the provisions of the PPDA by the COMPANY:

Storage Media
Lockable Archive Cabinet
Server
Domestic E-Mail Server
Computer
Book
Lockable Cabinet
Double-Lockable Cabinet in Controlled Area
Excel Programme
Operating Server
Software Programme
Overseas Server
EYS Folder
Archive Room
In a folder in the Purchasing Department
In a folder under the responsibility of the chemical engineer
In a folder in the Purchasing Department
In a folder in the Quality Department
Quality Folder
Online Backup Location
Online Backup Location - 2
In a folder in the Purchasing Department
In a folder in the Warehouse Department
In a folder in the Purchasing Department
Hard Disk
Encoded File
Archive Cabinet
Project Folder



PAGETEL Ltd. Şti.
İzmir- TÜRKİYE

KİŞİSEL VERİLERİN KORUNMASI VE İŞLENMESİ, KİŞİSEL VERİ SAKLAMA VE İMHA POLİTİKASI

Protection, Processing Storage and Destruction of Personal Data Policy
Kod/Code # FR-03.40

Tarih / Date :

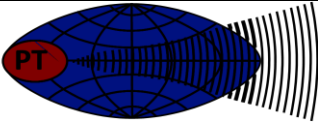
Sayfa / Page : 34 /
54

5. ŞİRKET TARAFINDAN İŞLENEN KİŞİSEL VERİLERİN SAHİPLERİNE İLİŞKİN KATEGORİZASYON

Kişisel Veri Sahibi Kategorisi	Açıklama
Çalışan Adayı	Şirkete herhangi bir yolla iş başvurusunda bulunmuş ya da özgeçmiş ve ilgili bilgilerini şirketimizin incelemesine açmış olan gerçek kişiler
Çalışan	Şirket ile arasında iş sözleşmesi olan gerçek kişiler
Tedarikçi Yetkilisi	Şirkete tedarik sözleşmesi ile bağlı bulunan şirketi temsile yetkili gerçek kişiler
Ziyaretçi	Şirketin sahip olduğu fiziksel yerleşkelere çeşitli amaçlarla girmiş olan veya internet sitelerimizi ziyaret eden gerçek kişiler
Ürün veya Hizmet Alan Kişi	Şirket ile herhangi bir sözleşmesel ilişkisi olup olmadığına bakılmaksızın Şirket iş birimlerinin yürüttüğü operasyonlar kapsamında Şirketin iş ilişkileri üzerinden kişisel verileri elde edilen gerçek kişiler
Tedarikçi Çalışanı	Şirkete tedarik sözleşmesi ile bağlı bulunan şirket ile aralarında iş sözleşmesi bulunan gerçek kişiler
Potansiyel Ürün veya Hizmet Alıcısı	Şirket ile ileride oluşacak hukuki ilişkiye temel olmak üzere Şirket iş birimlerinin yürüttüğü operasyonlar kapsamında Şirketin iş ilişkileri üzerinden kişisel verileri elde edilen gerçek kişiler
Dava, İcra Dosyası Tarafı	Dava, İcra Dosyası Tarafı
Tedarikçi	Tedarikçi
Kurumsal Müşteri Temsilcisi/Yetkilisi	Kurumsal Müşteri Temsilcisi/Yetkilisi
Dış Hizmet Alımı Yapılan Firma Temsilcileri	Dış Hizmet Alımı Yapılan Firma Temsilcileri
Kamu Görevlisi	Kamu Görevlisi
Müşteri Yetkilisi	Müşteri Yetkilisi
Çalışan Yakını	Çalışan Yakını
Çalışan Adayı Referansı	Çalışan Adayı Referansı

5. CATEGORISATION RELATED TO THE OWNERS OF PERSONAL DATE PROCESSED BY THE COMPANY

Personal Data Owner Category	Description
Employee Candidate	Natural persons who have filed job applications in any way or who have opened up their CVs and relevant data to the COMPANY for examination
Employee	Natural persons who have employment contracts with the COMPANY
Supplier's Authorised Official	Natural persons who are authorised to represent any company having a supply contract with the COMPANY
Visitor	Natural persons who have entered physical premises as owned by the COMPANY for various purposes or who visit our web sites
Product or Service Buyer	Notwithstanding whether or not they have any contractual relations with the COMPANY, natural persons whose personal data are obtained via the COMPANY's business relations within the scope of the operations carried out by the business units of the COMPANY
Supplier's Employee	Natural persons who have employment contracts with any company which has a supply contract with the COMPANY
Potential Product or Service Buyer	Natural persons whose personal data are obtained via the business relations of the COMPANY under the operations carried out by the business units of the COMPANY to be the basis of the legal relationship which will be established with the COMPANY in the future
Party to Litigation or Execution File	Party to Litigation or Execution File
Supplier	Supplier
Corporate Customer Representative/Authorised Official	Corporate Customer Representative/Authorised Official
Representatives of Companies from Which External Service Is Purchased	Representatives of Companies from Which External Service Is Purchased
Public Official	Public Official
Customer's Authorised Official	Customer's Authorised Official
Employee's Kinsman	Employee's Kinsman
Employee Candidate's Reference	Employee Candidate's Reference



PAGETEL Ltd. Şti.
İzmir- TÜRKİYE

KİŞİSEL VERİLERİN KORUNMASI VE İŞLENMESİ, KİŞİSEL VERİ SAKLAMA VE İMHA POLİTİKASI

Protection, Processing Storage and Destruction of Personal Data Policy
Kod/Code # FR-03.40

Tarih / Date :

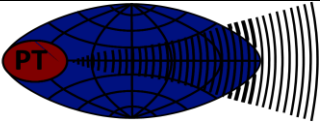
Sayfa / Page : 35 /
54

Aşağıdaki tabloda yukarıda belirtilen kişisel veri sahibi kategorileri ve bu kategoriler içerisindeki kişilerin hangi tip kişisel verilerin işlendiği detaylandırılmaktadır.

Categories of personal data owners and what types of personal data of those people in such categories are processed are detailed in the list in the following table.

Kişisel Veri Kategorizasyonu	İlgili Kişisel Verinin İlişkili Olduğu Veri Sahibi Kategorisi
Ad-Soyad	Çalışan Adayı Çalışan Tedarikçi Yetkilisi Dava, İcra Dosyası Tarafı Tedarikçi Ziyaretçi Ürün veya Hizmet Alan Kişi Kurumsal Müşteri Temsilcisi/Yetkilisi Dış Hizmet Alımı Yapılan Firma Temsilcileri Kamu Görevlisi Tedarikçi Çalışanı Potansiyel Ürün veya Hizmet Alıcısı Müşteri Yetkilisi Çalışan Yakını Çalışan Adayı Referansı
TC kimlik no v.b.	Çalışan Adayı Çalışan Dava, İcra Dosyası Tarafı Tedarikçi Tedarikçi Yetkilisi Ürün veya Hizmet Alan Kişi Kurumsal Müşteri Temsilcisi/Yetkilisi Çalışan Yakını
Telefon no v.b.	Çalışan Adayı Çalışan Tedarikçi Yetkilisi Ürün veya Hizmet Alan Kişi Tedarikçi Kurumsal Müşteri Temsilcisi/Yetkilisi Potansiyel Ürün veya Hizmet Alıcısı Tedarikçi Çalışanı Müşteri Yetkilisi Çalışan Adayı Referansı
E-posta adresi	Çalışan Tedarikçi Yetkilisi Ürün veya Hizmet Alan Kişi Tedarikçi Kurumsal Müşteri Temsilcisi/Yetkilisi Potansiyel Ürün veya Hizmet Alıcısı Tedarikçi Çalışanı Çalışan Adayı
İmza	Çalışan Tedarikçi Yetkilisi Ürün veya Hizmet Alan Kişi Tedarikçi Kurumsal Müşteri Temsilcisi/Yetkilisi Çalışan Adayı Tedarikçi Çalışanı Potansiyel Ürün veya Hizmet Alıcısı Ziyaretçi

Personal Data Categorisation	Data Owner Category with Which Relevant Personal Data Are Associated
First Name-Last Name	Employee Candidate Employee Supplier's Authorised Official Party to Litigation or Execution File Supplier Visitor Product or Service Buyer Corporate Customer Representative/Authorised Official Representatives of Companies from Which External Service Is Purchased Public Official Supplier's Employee Potential Product or Service Buyer Customer's Authorised Official Employee's Kinsman Employee Candidate's Reference
Personal identity nu, etc.	Employee Candidate Employee Party to Litigation or Execution File Supplier Supplier's Authorised Official Product or Service Buyer Corporate Customer Representative/Authorised Official Employee's Kinsman
Telephone no, etc.	Employee Candidate Employee Supplier's Authorised Official Product or Service Buyer Supplier Corporate Customer Representative/Authorised Official Potential Product or Service Buyer Supplier's Employee Customer's Authorised Official Employee Candidate's Reference
E-mail address	Employee Supplier's Authorised Official Product or Service Buyer Supplier Corporate Customer Representative/Authorised Official Potential Product or Service Buyer Supplier's Employee Employee Candidate
Signature	Employee Supplier's Authorised Official Product or Service Buyer Supplier Corporate Customer Representative/Authorised Official Employee Candidate Supplier's Employee Potential Product or Service Buyer Visitor



PAGETEL Ltd. Şti.
İzmir- TÜRKİYE

KİŞİSEL VERİLERİN KORUNMASI VE İŞLENMESİ, KİŞİSEL VERİ SAKLAMA VE İMHA POLİTİKASI

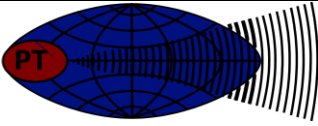
Protection, Processing Storage and Destruction of Personal Data Policy
Kod/Code # FR-03.40

Tarih / Date :

Sayfa / Page : 36 /
54

Görevi	Çalışan Kamu Görevlisi Tedarikçi Yetkilisi Çalışan Adayı
İletişim adresi	Tedarikçi Yetkilisi Dava, İcra Dosyası Tarafı Ziyaretçi Çalışan Ürün veya Hizmet Alan Kişi Tedarikçi Kurumsal Müşteri Temsilcisi/Yetkilisi Potansiyel Ürün veya Hizmet Alıcısı Tedarikçi Çalışanı Müşteri Yetkilisi Çalışan Adayı Çalışan Yakını Çalışan Adayı Referansı
Bordro bilgileri	Çalışan
İşe giriş-çıkış belgesi kayıtları	Çalışan
Adli makamlarla yazışmalardaki bilgiler	Çalışan
Çalışan Banka İban Numarası	Çalışan
Banka İban Numarası	Tedarikçi Tedarikçi Yetkilisi Ürün veya Hizmet Alan Kişi Potansiyel Ürün veya Hizmet Alıcısı Tedarikçi Çalışanı
Banka Bilgisi	Tedarikçi Tedarikçi Yetkilisi Kurumsal Müşteri Temsilcisi/Yetkilisi Ürün veya Hizmet Alan Kişi
Anne-Baba Adı	Çalışan Çalışan Yakını Çalışan Adayı
Doğum tarihi	Çalışan Çalışan Adayı Çalışan Yakını
Doğum yeri	Çalışan Çalışan Adayı Çalışan Yakını
Nüfusa Kayıtlı İl-İlçe	Çalışan
İşe Giriş-İşten Ayrılış Tarihleri	Çalışan
Araç Plakası	Ziyaretçi Çalışan

Position	Employee Public Official Supplier's Authorised Official Employee Candidate
Contact address	Supplier's Authorised Official Party to Litigation or Execution File Visitor Employee Product or Service Buyer Supplier Corporate Customer Representative/Authorised Official Potential Product or Service Buyer Supplier's Employee Customer's Authorised Official Employee Candidate Employee's Kinsman Employee Candidate's Reference
Payroll information	Employee
Recruitment/quitting document records	Employee
Information in correspondence with judicial authorities	Employee
Employee's IBAN	Employee
IBAN	Supplier Supplier's Authorised Official Product or Service Buyer Potential Product or Service Buyer Supplier's Employee
Bank Details	Supplier Supplier's Authorised Official Corporate Customer Representative/Authorised Official Product or Service Buyer
Parents' Names	Employee Employee's Kinsman Employee Candidate
Birth Date	Employee Employee Candidate Employee's Kinsman
Birth Place	Employee Employee Candidate Employee's Kinsman
Province-Town of Registration	Employee
Recruitment/Quitting Dates	Employee
Vehicle Registration Plate No	Visitor Employee



PAGETEL Ltd. Şti.
Izmir- TÜRKİYE

KİŞİSEL VERİLERİN KORUNMASI VE İŞLENMESİ, KİŞİSEL VERİ SAKLAMA VE İMHA POLİTİKASI

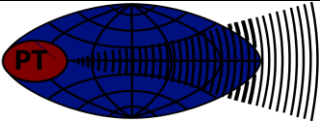
Protection, Processing Storage and Destruction of Personal Data Policy
Kod/Code # FR-03.40

Tarih / Date :

Sayfa / Page : 37 /
54

Çalışan ve ziyaretçilerin giriş çıkış kayıt bilgileri	Ziyaretçi
Medeni hali	Çalışan Çalışan Adayı
Nüfus cüzdanı seri sıra no	Çalışan
Cinsiyeti	Çalışan Çalışan Adayı Çalışan Yakını
Fotoğraf	Çalışan
Adres no	Çalışan Çalışan Adayı
Ceza mahkumiyetine ilişkin bilgiler	Çalışan Çalışan Adayı
Güvenlik tedbirlerine ilişkin bilgiler v.b.	Çalışan Çalışan Adayı
Fatura	Ürün veya Hizmet Alan Kişi Tedarikçi
Sipariş bilgisi	Ürün veya Hizmet Alan Kişi Tedarikçi Potansiyel Ürün veya Hizmet Alıcısı
Ticari, teknik, idari risklerin yönetilmesi için işlenen bilgiler v.b.	Ürün veya Hizmet Alan Kişi Tedarikçi Yetkilisi Tedarikçi
Bilanço bilgileri	Ürün veya Hizmet Alan Kişi
Finansal performans bilgileri	Ürün veya Hizmet Alan Kişi Tedarikçi Yetkilisi
Kredi ve risk bilgileri	Tedarikçi Yetkilisi Ürün veya Hizmet Alan Kişi Tedarikçi
Ücret Bilgisi	Çalışan Çalışan Adayı
Dava dosyasındaki bilgiler v.b.	Çalışan Çalışan Adayı
Engellilik durumuna ait bilgiler	Çalışan Çalışan Adayı
Cari Hesap Bilgisi	Ürün veya Hizmet Alan Kişi Tedarikçi
IP adresi bilgileri	Çalışan
Senet	Ürün veya Hizmet Alan Kişi Tedarikçi

Entrance/exit details of employees and visitors	Visitor
Civil status	Employee Employee Candidate
Identity card serial no	Employee
Gender	Employee Employee Candidate Employee's Kinsman
Photograph	Employee
Address no	Employee Employee Candidate
Information concerning criminal conviction	Employee Employee Candidate
Information concerning security measures, etc.	Employee Employee Candidate
Invoice	Product or Service Buyer Supplier
Purchase order information	Product or Service Buyer Supplier Potential Product or Service Buyer
Data processed to manage commercial, technical and administrative risks	Product or Service Buyer Supplier's Authorised Official Supplier
Balance sheet information	Product or Service Buyer
Financial performance information	Product or Service Buyer Supplier's Authorised Official
Credit and risk information	Supplier's Authorised Official Product or Service Buyer Supplier
Wage information	Employee Employee Candidate
Information in litigation file, etc.	Employee Employee Candidate
Information concerning handicaps	Employee Employee Candidate
Current Account information	Product or Service Buyer Supplier
IP address information	Employee
Promissory Notes	Product or Service Buyer Supplier



PAGETEL Ltd. Şti.
İzmir- TÜRKİYE

KİŞİSEL VERİLERİN KORUNMASI VE İŞLENMESİ, KİŞİSEL VERİ SAKLAMA VE İMHA POLİTİKASI

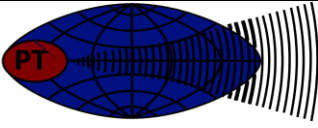
Protection, Processing Storage and Destruction of Personal Data Policy
Kod/Code # FR-03.40

Tarih / Date :

Sayfa / Page : 38 /
54

Çek Bilgileri	Ürün veya Hizmet Alan Kişi Tedarikçi
Talep bilgisi v.b.	Ürün veya Hizmet Alan Kişi Potansiyel Ürün veya Hizmet Alıcısı
Şifre ve parola bilgileri v.b.	Çalışan
Anne Kızlık Soyadı	Çalışan
Bulunduğu yerin konum bilgileri v.b.	Çalışan
Özgeçmiş bilgileri	Çalışan Çalışan Adayı
Kamera kayıtları v.b.	Çalışan Ziyaretçi
İnternet sitesi giriş çıkış bilgileri	Çalışan
Diploma bilgileri	Çalışan Çalışan Adayı
Gidilen kurslar	Çalışan Çalışan Adayı
Sertifikalar	Çalışan Çalışan Adayı
Transkript bilgileri v.b.	Çalışan Çalışan Adayı
Kan grubu bilgisi	Çalışan
Kişisel sağlık bilgileri	Çalışan Potansiyel Ürün veya Hizmet Alıcısı Tedarikçi Çalışanı Tedarikçi Yetkilisi Ziyaretçi
Parmak izi bilgileri	Çalışan
Yüz tanıma bilgileri v.b.	Çalışan
Eşinin Adı Soyadı	Çalışan
Çocukların Adı Soyadı	Çalışan
Çocukları Doğum Tarihi	Çalışan
Eşinin Doğum Tarihi	Çalışan
Çocuklarının Tc Nosu	Çalışan
Eşinin Tc Nosu	Çalışan
Anne-Baba TC Nosu	Çalışan
Mezuniyet Bilgisi	Çalışan Çalışan Adayı
Net Gelir ve Brüt Gelir Bilgisi	Çalışan Çalışan Yakını Çalışan Adayı
Ehliyet Bilgisi	Çalışan Çalışan Adayı
Askerlik Terhis Bilgisi	Çalışan Çalışan Adayı

Demand information, etc.	Product or Service Buyer Potential Product or Service Buyer
Password information, etc.	Employee
Mother's Nee	Employee
Position information of his/her location	Employee
CV information	Employee Employee Candidate
Camera recordings, etc.	Employee Visitor
Website log in/out information	Employee
Diploma information	Employee Employee Candidate
Courses attended	Employee Employee Candidate
Certificates	Employee Employee Candidate
Transcript information, etc.	Employee Employee Candidate
Blood type information	Employee
Personal health information	Employee Potential Product or Service Buyer Supplier's Employee Supplier's Authorised Official Visitor
Finger print information	Employee
Face recognition information, etc.	Employee
Spouse's First and Last Names	Employee
Children's First and Last Names	Employee
Children's Birth Dates	Employee
Spouse's Birth Date	Employee
Children's personal identity numbers	Employee
Spouse's personal identity number	Employee
Parents' personal identity numbers	Employee
Graduation information	Employee Employee Candidate
Net and Gross Income Information	Employee Employee's Kinsman Employee Candidate
Driver's license information	Employee Employee Candidate
Military service discharge information	Employee Employee Candidate



PAGETEL Ltd. Şti.
İzmir- TÜRKİYE

KİŞİSEL VERİLERİN KORUNMASI VE İŞLENMESİ, KİŞİSEL VERİ SAKLAMA VE İMHA POLİTİKASI

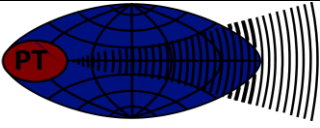
Protection, Processing Storage and Destruction of Personal Data Policy
Kod/Code # FR-03.40

Tarih / Date :

Sayfa / Page : 39 /
54

Yabancı Dil Bilgisi	Çalışan Çalışan Adayı
Mezun Olduğu Okul ve Bölüm Bilgisi	Çalışan Çalışan Adayı
Yaşı	Çalışan
Program Bilgisi	Çalışan Çalışan Adayı
Bilgi-Beceri	Çalışan Çalışan Adayı
Hedefler-Beklentiler-Başarılar	Çalışan Çalışan Adayı
Adayın Güçlü-Zayıf Yönleri	Çalışan Çalışan Adayı
Beden Dili	Çalışan Çalışan Adayı
Çalışan İşe Giriş Çıkış Saat Bilgisi	Çalışan
Evlilik Cüzdanı Fotokopisi	Çalışan
Disiplin soruşturması	Çalışan Çalışan Adayı
Görsel Kayıtlar	Çalışan Çalışan Adayı
Performans değerlendirme raporları v.b.	Çalışan
Mal bildirim bilgileri	Tedarikçi
Meslek içi eğitim bilgileri	Çalışan Çalışan Adayı
Mesleki Deneyim	Çalışan Çalışan Adayı
İşe giriş tarihi	Çalışan
Çalışan Beden Ölçüsü	Çalışan
Kişisel Gelişim	Çalışan Adayı
Özgüven	Çalışan Adayı
Sorumluluk	Çalışan Adayı
Sosyallik	Çalışan Adayı
Gelişim Potansiyeli	Çalışan Adayı
Cilt No-Sıra No-Birey Sıra No	Çalışan
Meslek	Çalışan

Foreign language information	Employee Employee Candidate
School and Department of Graduation Information	Employee Employee Candidate
Age	Employee
Programme Information	Employee Employee Candidate
Knowledge/Skills	Employee Employee Candidate
Goals-Expectations-Achievements	Employee Employee Candidate
Strengths-Weaknesses of Candidate	Employee Employee Candidate
Body Language	Employee Employee Candidate
Employee's Arrival at/Departure from Work Information	Employee
Photocopy of Marriage Certificate	Employee
Disciplinary investigation	Employee Employee Candidate
Visual Records	Employee Employee Candidate
Performance assessment reports, etc.	Employee
Declaration of assets information	Supplier
On-the-job training information	Employee Employee Candidate
Professional Experience	Employee Employee Candidate
Recruitment date	Employee
Employee's Body Size	Employee
Personal Development	Employee Candidate
Self-confidence	Employee Candidate
Responsibility	Employee Candidate
Sociability	Employee Candidate
Improvement Potential	Employee Candidate
Volume No-Pos. No-Individual Pos. No	Employee
Occupation	Employee



PAGETEL Ltd. Şti.
İzmir- TÜRKİYE

KİŞİSEL VERİLERİN KORUNMASI VE İŞLENMESİ, KİŞİSEL VERİ SAKLAMA VE İMHA POLİTİKASI

Protection, Processing Storage and Destruction of Personal Data Policy
Kod/Code # FR-03.40

Tarih / Date :

Sayfa / Page : 40 /
54

6. ŞİRKET TARAFINDAN KİŞİSEL VERİLERİN AKTARILDIĞI ÜÇÜNCÜ KİŞİLER VE AKTARILMA AMAÇLARI

Şirket, KVK Kanunu'nun 10. maddesine uygun olarak kişisel verilerin aktarıldığı kişi gruplarını kişisel veri sahibine bildirmektedir.

Şirket, KVK Kanunu'nun 8. ve 9. maddelerine uygun olarak (Bkz. Bölüm 3/Başlık 3.5) Politika ile yönetilen veri sahiplerinin kişisel verilerini aşağıda sıralanan kişi kategorilerine aktarılabilir:

- Yurtiçi Alıcılar: Yetkili Kamu Kurum ve Kuruluşları, Gerçek Kişiler veya Özel Hukuk Tüzel Kişileri, Tedarikçiler, İş Ortakları
- Yurtdışı Alıcılar: İştirakler ve Bağlı Ortaklıklar (Topluluk Şirketleri) , Tedarikçiler, İş Ortakları

Aktarımda bulunan yukarıda belirtilen kişilerin kapsamı ve veri aktarım amaçları aşağıda belirtilmektedir.

Veri Aktarımı Yapılabilecek Kişiler	Tanımı	Veri Aktarım Amacı
Yetkili Kamu Kurum ve Kuruluşları	İlgili mevzuat hükümlerine göre Şirketten bilgi ve belge almaya yetkili kamu kurum ve kuruluşları	Yasal Yükümlülük Mahkeme Emri İdare Talebi Veri Sorumlusunun Hukuki İş ve İşlemlerinin Takibi İlgili Kişi için Hizmet Sunumu Operasyonel İşlemler Bilgilendirme
Topluluk Şirketleri	Şirketin bağlı olduğu üst yapıya bağlı diğer Tüzel Kişiler	Bağlı ortaklıkları bilgilendirme Operasyonel İşlemler
Gerçek Kişiler veya Özel Hukuk Tüzel Kişileri	İlgili mevzuat hükümlerine göre Şirketten bilgi ve belge almaya yetkili özel hukuk kişileri veya gerçek kişiler	Veri Sorumlusunun Hukuki İş ve İşlemlerinin Takibi Operasyonel İşlemler Ödeme İşlemleri Bilgilendirme Denetim İşlemleri Yasal Yükümlülük İlgili Kişi için Hizmet Sunumu

6. THIRD PARTIES WHO ARE TRANSFERRED PERSONAL DATA BY THE COMPANY AND PURPOSES OF TRANSFER

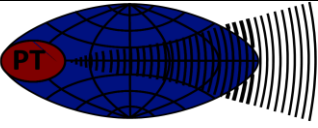
The COMPANY notifies the personal data owner of the groups to which personal data are transferred pursuant to the article 10 of the PPD Act.

The COMPANY may transfer the personal data of those data owners conducted by the Policy to the person categories as listed below pursuant to the article 8 and 9 of the PPD Act (see Section 3/paragraph 3.5):

- Domestic Buyers: Competent Public Organisations and Institutions, Natural Persons or Private Legal Entities, Suppliers, Business Partners
- Overseas Buyers: Affiliates and Subsidiaries (Group Companies), Suppliers, Business Partners

Scope of the abovementioned persons to whom data are transferred and data transfer purposes are specified below.

Persons to Whom Data May Be Transferred	Description	Data Transfer Purpose
Competent Public Organisations and Institutions	Public organisations and institutions authorised to obtain information and documentation from the COMPANY as per the provisions of the relevant regulations	Legal Obligation Court Order Administration's Claim Follow-up of Legal Affairs and Proceedings of Data Controller Service Delivery for Relevant Person Operational Procedures Information
Group Companies	Other Legal Entities affiliated to the higher organisation to which the COMPANY is affiliated	Provision of subsidiaries with information Operational Procedures
Natural Persons or Private Legal Entities	Private legal entities and natural persons authorised to obtain information and documentation from the COMPANY as per the provisions of the relevant regulations	Follow-up of Legal Affairs and Proceedings of Data Operational Procedures Payment Procedures Information Auditing Procedures Legal Obligation Service Delivery for Relevant Person



PAGETEL Ltd. Şti.
İzmir- TÜRKİYE

KİŞİSEL VERİLERİN KORUNMASI VE İŞLENMESİ, KİŞİSEL VERİ SAKLAMA VE İMHA POLİTİKASI

Protection, Processing Storage and Destruction of Personal Data Policy
Kod/Code # FR-03.40

Tarih / Date :

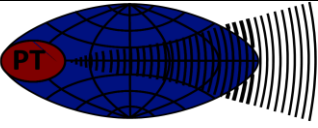
Sayfa / Page : 41 /
54

Tedarikçiler	Şirketin ticari faaliyetlerini yürütürken Şirketin emir ve talimatlarına uygun olarak sözleşme temelli olarak Şirkete hizmet sunan tarafları tanımlamaktadır.	Operasyonel İşlemler Bilgilendirme Ticari Amaç Sözleşme Yasal Yükümlülük İlgili Kişi için Hizmet Sunumu Ödeme İşlemleri
İştirakler ve Bağlı Ortaklıklar	Şirketin iştiraki veya hissedarı olduğu gerçek veya özel hukuk tüzel kişileri	Operasyonel İşlemler Bağlı ortaklıkları bilgilendirme Farkındalık Yaratma Bilgilendirme
İş Ortakları	Şirketin ticari faaliyetlerini birlikte yürüttüğü gerçek veya özel hukuk tüzel kişileri	Operasyonel İşlemler Sözleşme Ticari Amaç Bilgilendirme

Şirket tarafından gerçekleştirilen aktarımlarda Politika'nın 2. ve 3. Bölümlerinde düzenlenmiş hususlara uygun olarak hareket edilmektedir.

Suppliers	Parties that provide the COMPANY with services on contract basis in compliance with the orders and instructions of the COMPANY while the COMPANY carries out its business operations	Operational Procedures Information Commercial Purposes Contract Legal Obligation Service Delivery for Relevant Person Payment Procedures
Affiliates and Subsidiaries	Natural persons or private legal entities in which the COMPANY is an affiliate or shareholder	Operational Procedures Provision of subsidiaries with information Awareness Raising Information
Business Partners	Natural persons or private legal entities with which the COMPANY carries out its business operations	Operational Procedures Contract Commercial Purposes Information

In transfers carried out by the COMPANY, action is taken pursuant to the issues regulated in the Sections 2 and 3 of the Policy.



PAGETEL Ltd. Şti.
İzmir- TÜRKİYE

KİŞİSEL VERİLERİN KORUNMASI VE İŞLENMESİ, KİŞİSEL VERİ SAKLAMA VE İMHA POLİTİKASI

Protection, Processing Storage and Destruction of Personal Data Policy
Kod/Code # FR-03.40

Tarih / Date :

Sayfa / Page : 42 /
54

7. KİŞİSEL VERİLERİN KANUNDAKİ İŞLEME ŞARTLARINA DAYALI VE BU ŞARTLARLA SINIRLI OLARAK İŞLENMESİ

Şirket, KVK Kanunu'nun 10. maddesine uygun olarak işlediği kişisel veriler hakkında kişisel veri sahibini aydınlatmaktadır.

7.1. Kişisel Verilerin ve Özel Nitelikli Kişisel Verilerin İşlenmesi

7.1.1. Kişisel Verilerin İşlenmesi

Kişisel veri sahibinin açık rıza vermesi, kişisel verilerin hukuka uygun olarak işlenmesini mümkün kılan hukuki dayanaklardan yalnızca bir tanesidir. Açık rıza dışında, aşağıda yazan diğer şartlardan birinin varlığı durumunda da kişisel veriler işlenebilir. Kişisel veri işleme faaliyetinin dayanağı aşağıda belirtilen şartlardan yalnızca biri olabildiği gibi bu şartlardan birden fazlası da aynı kişisel veri işleme faaliyetinin dayanağı olabilir. İşlenen verilerin özel nitelikli kişisel veri olması halinde; aşağıda bu bölüm altında 7.1.2. başlığı içerisinde yer alan şartlar uygulanır.

Şirket tarafından kişisel verilerin işlenmesine yönelik hukuki dayanaklar farklılık gösterse de, her türlü kişisel veri işleme faaliyetinde KVK Kanunu'nun 4. maddesinde belirtilen (Bkz.3.1.) genel ilkelere uygun olarak hareket edilmektedir.

7.1.1.1. Kişisel Veri Sahibinin Açık Rızasının Bulunması

Kişisel verilerin işleme şartlarından biri sahibinin açık rızasıdır. Kişisel veri sahibinin açık rızası belirli bir konuya ilişkin, bilgilendirilmeye dayalı olarak ve özgür iradeyle açıklanmalıdır.

Kişisel verilerin elde edilme sebeplerine yönelik işleme amacının (birincil işleme) dışındaki kişisel veri işleme faaliyetleri için (ikincil işleme) işbu başlığın 7.1.1.2- 7.1.1.8'de yer alan şartlardan en az biri aranmakta; bu şartlardan biri yok ise, Şirket tarafından bu kişisel veri işleme faaliyetleri kişisel veri sahibinin bu işleme faaliyetlerine yönelik açık rızasına dayalı olarak gerçekleştirilmektedir.

Kişisel verilerin, kişisel veri sahibinin açık rıza vermesine bağlı olarak işlenmesi için, kişisel veri sahiplerinin ilgili yöntemler ile açık rızaları alınmaktadır.

7.1.1.2. Kanunlarda Açıkça Öngörülmesi

Veri sahibinin kişisel verileri, kanunda açıkça öngörülmesi halinde hukuka uygun olarak işlenebilecektir.

7. PROCESSING OF PERSONAL DATA BASING ON AND LIMITED TO THE PROCESSING CONDITIONS IN THE ACT

The COMPANY clarifies the personal data owner about the personal data it processes pursuant to the article 10 of the PPD Act.

7.1. Processing of Personal Data and Sensitive Personal Data

7.1.1. Processing of Personal Data

Personal data owner's giving his/her explicit consent is only one of the legal bases which make it possible to process personal data in a legal manner. Except explicit consent, personal data may also be processed in case of the existence of any of the following conditions. While the basis of personal data processing activity may only be one of the conditions as listed below, more than one of those conditions may also be the basis of the same personal data processing activity. In case the personal data so processed are sensitive personal data, the conditions as contained in the subparagraph 7.1.2 in this section are applied.

Even if the legal bases for the processing of personal data by the COMPANY vary, action is taken pursuant to the general principles as stipulated in the article 4 of the PPD Act in any and all personal data processing activities (see 3.1).

7.1.1.1. Existence of Personal Data Owner's Explicit Consent

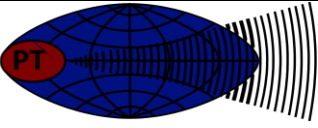
One of the conditions for processing personal data is the explicit consent of the owner thereof. Explicit consent of the personal data owner should be disclosed on a certain matter, on the basis of information and on free will.

For any personal data processing activities (secondary processing) other than the processing purpose (primary processing) for the reasons of obtaining personal data, at least one of the conditions as contained in the subparagraphs 7.1.1.2 – 7.1.1.8 of this paragraph is required and if one of these conditions does not exist, such personal data processing activities are carried out on the basis of the explicit consent of the personal data owner by the COMPANY.

Explicit consents of the personal data owners are obtained by the relevant methods so that personal data will be processed on the basis of the personal data owner's giving his/her explicit consent.

7.1.1.2. Explicit Stipulation by Laws

Personal data of the data owner may be legally processed in case



PAGETEL Ltd. Şti.
Izmir- TÜRKİYE

KİŞİSEL VERİLERİN KORUNMASI VE İŞLENMESİ, KİŞİSEL VERİ SAKLAMA VE İMHA POLİTİKASI

Protection, Processing Storage and Destruction of Personal Data Policy
Kod/Code # FR-03.40

Tarih / Date :

Sayfa / Page : 43 /
54

7.1.1.4. Sözleşmenin Kurulması veya İfasıyla Doğrudan İlgili Olması

Bir sözleşmenin kurulması veya ifasıyla doğrudan doğruya ilgili olması kaydıyla, sözleşmenin taraflarına ait kişisel verilerin işlenmesinin gerekli olması halinde kişisel verilerin işlenmesi mümkündür.

7.1.1.5. Şirketin Hukuki Yükümlülüğünü Yerine Getirmesi

Şirket, veri sorumlusu olarak hukuki yükümlülüklerini yerine getirmesi için işlemenin zorunlu olması halinde veri sahibinin kişisel verileri işlenebilecektir.

7.1.1.6. Kişisel veri Sahibinin Kişisel Verisini Alenileştirmesi

Veri sahibinin, kişisel verisini kendisi tarafından alenileştirilmiş olması halinde ilgili kişisel veriler işlenebilecektir.

7.1.1.7. Bir Hakkın Tesisi veya Korunması için Veri İşlemenin Zorunlu Olması

Bir hakkın tesisi, kullanılması veya korunması için veri işlemenin zorunlu olması halinde kişisel veri sahibinin kişisel verileri işlenebilecektir.

7.1.1.8. Şirketin Meşru Menfaati için Veri İşlemenin Zorunlu Olması

Kişisel veri sahibinin temel hak ve özgürlüklerine zarar vermemek kaydıyla Şirketin meşru menfaatleri için veri işlenmesinin zorunlu olması halinde veri verileri işlenebilecektir.

7.1.1.4. Direct Relation to the Execution or Performance of a Contract

Provided that they are related to the execution or performance of a contract, it is possible to process personal data in case personal data belonging to the contractual parties are required to be processed.

7.1.1.5. COMPANY's Fulfilment of Its Legal Obligation

Personal data of the data owner may be processed in case processing is necessary so that the COMPANY will fulfil its legal obligations in its capacity as the data controller.

7.1.1.6. Personal Data Owner's Making His/Her Personal Data Public

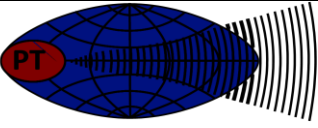
In case the data owner has made his/her personal data public, relevant personal data may be processed.

7.1.1.7. Data Processing Being Necessary for the Creation or Protection of Any Right

In case data processing is necessary in order to create, exercise or protect any right, personal data of the data owner may be processed.

7.1.1.8. Data Processing Being Necessary for the Legitimate Interest of the COMPANY

Provided that the basic rights and freedoms of the personal data owner are not prejudiced, personal data may be processed in case data processing is necessary for the legitimate interests of the COMPANY.



PAGETEL Ltd. Şti.
İzmir- TÜRKİYE

KİŞİSEL VERİLERİN KORUNMASI VE İŞLENMESİ, KİŞİSEL VERİ SAKLAMA VE İMHA POLİTİKASI

Protection, Processing Storage and Destruction of Personal Data Policy
Kod/Code # FR-03.40

Tarih / Date :

Sayfa / Page : 44 /
54

7.1.2. Özel Nitelikli Kişisel Verilerin İşlenmesi

Şirket tarafından; özel nitelikli kişisel veriler kişisel veri sahibinin açık rızası yok ise ancak, KVK Kurulu tarafından belirlenecek olan yeterli önlemlerin alınması kaydıyla aşağıdaki durumlarda işlenmektedir:

- Kişisel veri sahibinin sağlığı ve cinsel hayatı dışındaki özel nitelikli kişisel veriler, kanunlarda öngörülen hallerde,
- Kişisel veri sahibinin sağlığına ve cinsel hayatına ilişkin özel nitelikli kişisel verileri ise ancak kamu sağlığının korunması, koruyucu hekimlik, tıbbi teşhis, tedavi ve bakım hizmetlerinin yürütülmesi, sağlık hizmetleri ile finansmanının planlanması ve yönetimi amacıyla, sır saklama yükümlülüğü altında bulunan kişiler veya yetkili kurum ve kuruluşlar tarafından.

7.2. Bina, Tesis Girişleri ile Bina Tesis İçerisinde Yapılan Kişisel Veri İşleme Faaliyetleri

Şirket tarafından bina tesis girişlerinde ve tesis içerisinde yapılan kişisel veri işleme faaliyetleri, Anayasa'ya, KVK Kanunu'na ve ilgili diğer mevzuata uygun bir biçimde yürütülmektedir.

Şirket tarafından güvenliğin sağlanması amacıyla, Şirket binalarında ve tesislerinde güvenlik kamerasıyla izleme faaliyeti ile misafir giriş çıkışlarının takibine yönelik kişisel veri işleme faaliyetinde bulunmaktadır.

Güvenlik kameraları kullanılması ve misafir giriş çıkışlarının kayıt altına alınması yoluyla Şirket tarafından kişisel veri işleme faaliyeti yürütülmüş olmaktadır.

7.2.1. Şirket Bina, Tesis Girişlerinde ve İçerisinde Yürütülen Kamera ile İzleme Faaliyeti

Bu bölümde Şirketin kamera ile izleme sistemine ilişkin açıklamalar yapılacak ve kişisel verilerin, gizliliğinin ve kişinin temel haklarının nasıl korumaya alındığına ilişkin bilgilendirme yapılacaktır.

Şirket, güvenlik kamerası ile izleme faaliyeti kapsamında; şirketin ve diğer kişilerin güvenliğini sağlamaya ilişkin menfaatlerini korumak gibi amaçlar taşımaktadır.

7.1.2. Processing of Sensitive Personal Data

In case of the absence of the explicit consent of the personal data owner, sensitive personal data may only be processed in the following cases provided that any adequate measures to be identified by the PPD Committee will be taken:

- Sensitive personal data except the health and sexual life of the personal data owner: in cases as stipulated in laws;
- Sensitive personal data concerning the health and sexual life of the personal data owner: for the purposes of the protection of public health, implementation of preventive medicine, medical diagnosis, treatment and care services and planning and management of the healthcare services and financing thereof by those individuals or competent organisations or institutions obliged to keep secrets.

7.2. Personal Data Processing Activities Carried out at Building and Facility Entrances and Inside the Buildings and Facilities

Personal data processing activities carried out at the entrances to and inside of the buildings and facilities are carried out pursuant to the Constitution, PPD Act and other relevant regulations.

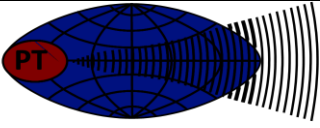
The COMPANY carries out surveillance activities by means of security cameras as well as personal data processing activities for watching the entries and exits of visitors at its buildings and facilities.

The COMPANY carries out personal data processing activities by using security cameras and recording visitor entries and exits.

7.2.1. Surveillance Activities Carried out by Means of Cameras at the Entrances to and Inside of the Buildings and Facilities of the COMPANY

In this section, explanations will be given about the camera surveillance system of the COMPANY and information will be provided as to how confidentiality of personal data and person's basic rights are protected.

The COMPANY has such purposes as protecting the COMPANY's interests related to the provision of the security of the COMPANY and other people within the scope of its surveillance activities by means of security cameras.



PAGETEL Ltd. Şti.
İzmir- TÜRKİYE

KİŞİSEL VERİLERİN KORUNMASI VE İŞLENMESİ, KİŞİSEL VERİ SAKLAMA VE İMHA POLİTİKASI

Protection, Processing Storage and Destruction of Personal Data Policy
Kod/Code # FR-03.40

Tarih / Date :

Sayfa / Page : 45 /
54

7.2.2. KVK Hukukuna Göre Güvenlik Kamerası ile İzleme Faaliyeti Yürütülmesi

Şirket tarafından güvenlik amacıyla kamera ile izleme faaliyeti yürütülmesinde KVK Kanunu'nda yer alan düzenlemelere uygun hareket edilmektedir. Şirket, bina ve tesislerinde güvenliğin sağlanması amacıyla, yürürlükte bulunan ilgili mevzuatta öngörülen amaçlarla ve KVK Kanunu'nda sayılan kişisel veri işleme şartlarına uygun olarak güvenlik kamerası izleme faaliyetinde bulunmaktadır.

7.2.3. Kamera ile İzleme Faaliyetinin Duyurulması

Şirket tarafından KVK Kanunu'nun 10. Maddesine uygun olarak, kişisel veri sahibi aydınlatılmaktadır. Şirket, genel hususlara ilişkin olarak yaptığı aydınlatmanın (Bkz. Bölüm 3/Başlık 3.3) kamera ile izleme faaliyetine ilişkin birden fazla yöntem ile bildirimde bulunmaktadır. Böylelikle, kişisel veri sahibinin temel hak ve özgürlüklerine zarar verilmesinin engellenmesi, şeffaflığın ve kişisel veri sahibinin aydınlatılmasının sağlanması amaçlanmaktadır.

Şirket tarafından kamera ile izleme faaliyetine yönelik olarak; Şirket internet sitesinde işbu Politika yayımlanmakta (çevrimiçi politika düzenlemesi) ve izlemenin yapıldığı alanların girişlerine izleme yapılacağına ilişkin bildirim yazısı asılmaktadır (yerinde aydınlatma).

7.2.4. Kamera ile İzleme Faaliyetinin Yürütülme Amacı ve Amaçla Sınırlılık

Şirket, KVK Kanunu'nun 4. maddesine uygun olarak, kişisel verileri işlendikleri amaçla bağlantılı, sınırlı ve ölçülü bir biçimde işlemektedir.

Şirket tarafından video kamera ile izleme faaliyetinin sürdürülmesindeki amaç bu Politika'da sayılan amaçlarla sınırlıdır. Bu doğrultuda, güvenlik kameralarının izleme alanları, sayısı ve ne zaman izleme yapılacağı, güvenlik amacına ulaşmak için yeterli ve bu amaçla sınırlı olarak uygulamaya alınmaktadır. Kişinin mahremiyetini güvenlik amaçlarını aşan şekilde müdahale sonucu doğurabilecek alanlarda (örneğin, tuvaletler) izlemeye tabi tutulmamaktadır.

7.2.2. Implementation of Surveillance Activity by Means of Security Cameras as per the PPD Act

In the implementation of the camera surveillance activity for security purposes by the COMPANY, action is taken pursuant to the stipulations as contained in the PPD Act. The COMPANY carries out camera surveillance activities for the purposes stipulated in the relevant regulations in effect and personal data processing conditions listed in the PPD Act in order to provide security at its buildings and facilities.

7.2.3. Notification of the Camera Surveillance Activity

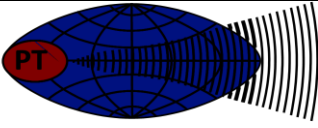
Personal data owner is provided with clarification as per the article 10 of the PPD Act by the COMPANY. The COMPANY makes notices by more than one method concerning the camera surveillance activity in the clarification which it provides about general issues (see Section 3 paragraph 3.3). Thus, it is aimed at preventing the personal data owner's basic rights and freedoms from being prejudiced and ensuring transparency and providing the personal data owner with clarification.

In connection with its camera surveillance activity, the COMPANY publishes this Policy in its website (online Policy edition) and posts notices as to the surveillance at the entrances to the areas where surveillance will take place (on-site surveillance).

7.2.4. Purpose of the Implementation of Camera Surveillance Activity and Limitation by Purpose

The COMPANY processes personal data in a limited and moderate manner related to the purposes for which they are processed pursuant to the article 4 of the PPD Act.

Purpose for the COMPANY's maintaining the camera surveillance activity is limited to those as listed in this Policy. In this context, surveillance areas, number and time to carry out surveillance are put into practice in an adequate manner to achieve the security purposes and limited to such purposes. Any areas (for instance, restrooms) are not subjected to camera surveillance which may result in intervention with the person's privacy to exceed the purposes of security.



PAGETEL Ltd. Şti.
İzmir- TÜRKİYE

KİŞİSEL VERİLERİN KORUNMASI VE İŞLENMESİ, KİŞİSEL VERİ SAKLAMA VE İMHA POLİTİKASI

Protection, Processing Storage and Destruction of Personal Data Policy
Kod/Code # FR-03.40

Tarih / Date :

Sayfa / Page : 46 /
54

7.2.5. Elde Edilen Verilerin Güvenliğinin Sağlanması

Şirket tarafından KVK Kanunu'nun 12. maddesine uygun olarak, kamera ile izleme faaliyeti sonucunda elde edilen kişisel verilerin güvenliğinin sağlanması için gerekli teknik ve idari tedbirler alınmaktadır. (Bkz. 2.1)

7.2.6. Kamera ile İzleme Faaliyeti ile Elde Edilen Kişisel Verilerin Muhafaza Süresi

Şirketin, kamera ile izleme faaliyeti ile elde edilen kişisel verileri muhafaza süresi ile ilgili ayrıntılı bilgiye bu Politika'nın Kişisel Verilerin Saklanması Süreleri isimli 4.3. maddesinde yer verilmiştir.

7.2.7. İzleme Sonucunda Elde Edilen Bilgilere Kimlerin Erişebileceği ve Bu Bilgilerin Kimlere Aktarıldığı

Canlı kamera görüntüleri ile dijital ortamda kaydedilen ve muhafaza edilen kayıtlara yalnızca sınırlı sayıda Şirket çalışanının erişimi bulunmaktadır. Kayıtlara erişimi olan sınırlı sayıda kişi gizlilik taahhütnamesi ile eriştiği verilerin gizliliğini koruyacağını beyan etmektedir.

7.3. Şirket Bina, Tesis Girişlerinde ve İçerisinde Yürütülen Misafir Giriş Çıkışlarının Takibi

Şirket tarafından; güvenliğin sağlanması ve bu Politika'da belirtilen amaçlarla, Şirket binalarında ve tesislerinde misafir giriş çıkışlarının takibine yönelik kişisel veri işleme faaliyetinde bulunmaktadır.

Misafir olarak Şirket binalarına gelen kişilerin isim ve soyadları elde edilirken ya da Şirket nezdinde asılan ya da diğer şekillerde misafirlerin erişimine sunulan metinler aracılığıyla söz konusu kişisel veri sahipleri bu kapsamda aydınlatılmaktadırlar. Misafir giriş-çıkış takibi yapılması amacıyla elde edilen veriler yalnızca bu amaçla işlenmekte ve ilgili kişisel veriler fiziki ortamda veri kayıt sistemine kaydedilmektedir.

7.2.5. Provision of Security of Data Obtained

The COMPANY takes any and all necessary technical and administrative measures in order to provide the security of the personal data obtained as a result of the camera surveillance activity pursuant to the article 12 of the PPD Act (see 2.1).

7.2.6. Storage Period of Personal Data Obtained through Camera Surveillance Activity

Detailed information concerning the storage period of the personal data obtained through the camera surveillance activity by the COMPANY is provided in the paragraph 4.3 entitled "Storage Periods of Personal Data" of this Policy.

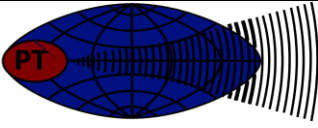
7.2.7. Accessibility of Information Obtained as a Result of Surveillance and to Whom Such Data Are Transferred

Only a limited number of COMPANY employees may have access to live camera images and the images recorded and stored in digital media. Limited number of people who have access to the recordings declare that they will protect the confidentiality of the data to which they access under a confidentiality commitment.

7.3. Tracking Visitor Entries and Exits at Entrances to and Inside of Buildings and Facilities

The COMPANY carries out data processing activities for tracking the visitor entries and exits at the buildings and facilities of the COMPANY for the provision of security and for the purposes as set forth in this Policy by the COMPANY.

While obtaining first and last names of the people who arrive at the COMPANY buildings as visitors or through the texts posted at the COMPANY or provided to be accessed by the visitors in any other manners, the said personal data owners are provided with clarification in this context. Data obtained for the purpose of keeping track of the visitor entries/exits are only processed for this purpose and relevant personal data are recorded in the data recording system in physical media.



PAGETEL Ltd. Şti.
İzmir- TÜRKİYE

KİŞİSEL VERİLERİN KORUNMASI VE İŞLENMESİ, KİŞİSEL VERİ SAKLAMA VE İMHA POLİTİKASI

Protection, Processing Storage and Destruction of Personal Data Policy
Kod/Code # FR-03.40

Tarih / Date :

Sayfa / Page : 47 /
54

7.4. Şirket Bina ve Tesislerinde Ziyaretçilerimize Sağlanan İnternet Erişimlerine İlişkin Kayıtların Saklanması

Şirket tarafından güvenliğin sağlanması ve bu Politika'da belirtilen amaçlarla; Şirket tarafından bina ve tesislerimiz içerisinde kaldığınız süre boyunca talep eden Ziyaretçi'lerimize internet erişimi sağlanabilmektedir. Bu durumda internet erişimlerimize ilişkin log kayıtları 5651 Sayılı Kanun ve bu Kanuna göre düzenlenmiş olan mevzuatın amir hükümlerine göre kayıt altına alınmakta; bu kayıtlar ancak yetkili kamu kurum ve kuruluşları tarafından talep edilmesi veya Şirket içinde gerçekleştirilecek denetim süreçlerinde ilgili hukuki yükümlülüğümüzü yerine getirmek amacıyla işlenmektedir.

Bu çerçevede elde edilen log kayıtlarına yalnızca sınırlı sayıda Şirket çalışanının erişimi bulunmaktadır. Bahsi geçen kayıtlara erişimi olan Şirket çalışanları bu kayıtları yalnızca yetkili kamu kurum ve kuruluşundan gelen talep veya denetim süreçlerinde kullanmak üzere erişmekte ve hukuken yetkili olan kişilerle paylaşmaktadır. Kayıtlara erişimi olan sınırlı sayıda kişi gizlilik taahhütname ile eriştiği verilerin gizliliğini koruyacağını beyan etmektedir.

8. KİŞİSEL VERİLERİN SİLİNMESİ, YOK EDİLMESİ VE ANONİMLEŞTİRİLMESİ ŞARTLARI

Şirket, Türk Ceza Kanunu'nun 138. maddesinde ve KVK Kanunu'nun 7. maddesinde düzenlendiği üzere ilgili kanun hükümlerine uygun olarak işlenmiş olmasına rağmen, işlenmesini gerektiren sebeplerin ortadan kalkması hâlinde Şirketin kendi kararına istinaden veya kişisel veri sahibinin talebi üzerine kişisel veriler silinir, yok edilir veya anonim hâle getirilir.

Bu çerçevede:

- Mevzuatın değişmesi veya ilgası,
- İşlemeye esas sözleşmenin sona ermesi veya hükümsüzlüğü,
- İşlenme amaçlarının ve şartlarının ortadan kalkması,
- Açık rızaya bağlı işleme faaliyetlerinde rızanın geri alınması,
- Veri Sahibinin silme-yok etme-anonim hale getirme başvurusunda bulunması ve bu başvurunun kabulü,
- Veri Sahibinin başvuruda bulunması ve bu başvurunun reddi neticesinde Kişisel Verileri Koruma Kurulu tarafından verilecek talebin karşılanması gerektiğine ilişkin karar,
- Saklama süresinin sona ermesi,
- Şirket bünyesinde gerçekleştirilen periyodik imha işlemleri,

neticesinde Şirketimiz topladığı Kişisel Verileri silmekte, imha etmekte veya anonim hale getirmektedir.

7.4. Storage of the Records Concerning the Internet Access with Which Visitors Are Provided at the Buildings and Facilities of the COMPANY

For the purposes of the provision of security by the COMPANY and those set forth in this Policy, the COMPANY may provide any requesting visitors with internet access during the period of time they stay in our buildings and facilities. In such a case, log records related to your internet accesses are entered in records as per the Act No. 5651 and the mandatory provisions of any regulations issued under such Act and such records are only processed in order to fulfil our relevant legal obligations upon request from any competent public organisations and institutions or during the audit processes to be carried out in the COMPANY.

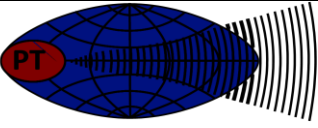
Only a limited number of the COMPANY employees have access to the log records obtained in this context. Those COMPANY employees who have access to the abovementioned records only access to such records to be used in case of requests from or audit processes of any competent public organisations and institutions and such records are shared with those people who are legally authorised. Limited number of people who have access to the records declare that they will maintain the privacy of any data to which they have access under a confidentiality commitment.

8. CONDITIONS FOR THE DELETION, DESTRUCTION AND ANONYMIZATION OF PERSONAL DATA

Personal data are deleted, destroyed or anonymized on the basis of the COMPANY's own decision or upon the request of the personal data owner in case the reasons for the processing of personal data cease to exist despite they have been processed pursuant to the legal provisions as provided in the article 138 of the Turkish Criminal Code and in the article 7 of the PPD Act by the COMPANY.

In this context, the COMPANY deletes, destroys or anonymizes the collected Personal Data as a result of

- amendment to or abrogation of legislation;
- termination or invalidity of the contract on which processing is based;
- cessation of the existence of purposes of and reasons for processing;
- revocation of consent in processing activities based on explicit consent;
- Data Owner's application for deletion, destruction and anonymization and acceptance of such application;
- Data Owner's application and dismissal of such



PAGETEL Ltd. Şti.
Izmir- TÜRKİYE

KİŞİSEL VERİLERİN KORUNMASI VE İŞLENMESİ, KİŞİSEL VERİ SAKLAMA VE İMHA POLİTİKASI

Protection, Processing Storage and Destruction of Personal Data Policy
Kod/Code # FR-03.40

Tarih / Date :

Sayfa / Page : 48 /
54

8.1. Kişisel Verilerin Silinmesi, Yok Edilmesi ve Anonimleştirilmesi Teknikleri

Şirketimiz, topladığı Kişisel Verileri, işlenmesini gerektiren sebeplerin ortadan kalkması hâlinde kendiliğinden veya Veri Sahibinin talebi üzerine silmekte, yok etmekte veya anonim hale getirmektedir. Kanun'un 28. maddesine uyarınca ise, anonim hale getirilmiş olan kişisel veriler araştırma, planlama ve istatistik gibi amaçlarla işlenebilmektedir. Anonimleştirme sonrasında gerçekleştirilen bu tür işlemler Kanun kapsamı dışında olup, bu durumda kişisel Veri Sahibinin açık rızası aranmamaktadır.

Bu çerçevede, Şirketimiz tarafından, aşağıda belirtilen silme, imha etme veya anonim hale getirme usullerinden biri veya birkaçı seçilerek, amaca en uygun yöntem izlenmektedir:

8.1.1. Dijital Belgenin İmhası

Şirket bünyesinde dijital ortamlarda üretilen veya elde edilen Kişisel Veri içeren Dijital Belgeler, İlgili Kullanıcılar için hiçbir şekilde erişilemez ve tekrar kullanılamaz hale getirilecek biçimde kalıcı olarak silinmektedir.

8.1.2. Fiziki Belgenin İmhası

Şirketimizce toplanan ve veri kayıt sistemlerimizin parçası olmakla birlikte otomatik olmayan yollarla işlediğimiz Kişisel Veriler, buldukları ortamın (kağıt, mikrofiş) üzerindeki Kişisel Verinin sonradan kullanılmasına imkan vermeyecek biçimde fiziksel olarak yok edilmesi suretiyle de yok edilebilmektedir.

8.1.3. Veri Tabanından Silme

Şirketimizde, veri tabanında muhafaza edilen Kişisel Veriler, İlgili Kullanıcılar için hiçbir şekilde erişilemez ve tekrar kullanılamaz hale getirilecek biçimde ilgili veri tabanından silinmektedir.

Kullandığımız Ticari Paket Programlar, İnsan Kaynakları Programları, SQL veri tabanları gibi elektronik kayıt ortamlarına silme komutu verilerek verilerin silinmesi, merkezi sunucumuzda yer alan dosyalara veya dosyaların bulunduğu dizin üzerinde İlgili Kullanıcıların erişim haklarının kaldırılması; veri tabanlarında ilgili satırların veri tabanı komutları ile silinmesi veya taşınabilir medyada (USB, HDD, vb.) bulunan Kişisel Verilerin uygun yazılımlar kullanılarak silinmesi suretiyle veriler silinebilmektedir.

8.1. Deletion, Destruction and Anonymization Techniques of Personal Data

The COMPANY deletes, destroys or anonymizes any Personal Data which it has collected in an automatic manner or upon the Data Owner's request in case the reasons requiring the processing of Personal Data cease to exist. But, as per the article 28 of the Act, any anonymized personal data may be processed for such purposes as research, planning and statistics. Processing of his kind carried out after anonymization is excluded from the Act and Data Owner's explicit consent is not required in this case.

In this context, the COMPANY pursues the most appropriate method by selecting one or some of the deletion, destruction or anonymization procedures as described below:

8.1.1. Destruction of Digital Documents

Digital Documents containing Personal Data generated or obtained on digital media in the COMPANY are permanently deleted in a manner which will be inaccessible and reusable by any Related Users.

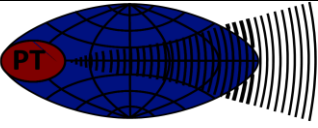
8.1.2. Destruction of Physical Documents

Personal Data that have been collected by the COMPANY and that are part of our data recording systems but processed by non-automatic ways may be destroyed by physically destroying the Personal data on the media in which they are stored (hardcopy, microfiche) in a manner which will not allow the same to be re-used.

8.1.3. Deletion from Database

Personal Data stored in the database in the COMPANY are deleted from the database in a manner in which they will not be by any means accessible and reusable by any Related Users.

Data may be deleted by deleting the data by giving a deletion prompt to such electronic recording media as Commercial Package Programmes, Human Resources Programmes, SQL databases, etc. we use; by removing the Related Users' rights of access to the files contained in our central server or the directory where such files are available; by deleting any relevant lines available in databases using database prompts or by deleting any Personal data contained in portable media (USB, HDD, etc.) by using proper software.



PAGETEL Ltd. Şti.
Izmir- TÜRKİYE

KİŞİSEL VERİLERİN KORUNMASI VE İŞLENMESİ, KİŞİSEL VERİ SAKLAMA VE İMHA POLİTİKASI

Protection, Processing Storage and Destruction of Personal Data Policy
Kod/Code # FR-03.40

Tarih / Date :

Sayfa / Page : 49 /
54

Ancak, bazı Kişisel Verilerin silinmesi sebebiyle diğer bir kısım verilere de sistemde erişimin mümkün olmadığı hallerde, silmeye konu Kişisel Veriler ilgili Veri Sahibi ile ilişkilendirilemeyecek duruma getirilerek arşivlenebilmektedir; bu durumda da ilgili Kişisel Veriler silinmiş sayılmaktadır. Böyle durumlarda Şirketimiz, Kişisel Verilere yalnızca yetkili kişiler tarafından erişilmesini sağlayacak şekilde gerekli her türlü teknik ve idari tedbiri almaktadır.

8.1.4. Kullanılan Yazılım Programlarından Silme

Şirketimiz bünyesindeki dijital ortamlarda muhafaza edilen Kişisel Veriler, ilgili Kullanıcılar için hiçbir şekilde erişilemez ve tekrar kullanılamaz hale getirilecek biçimde ilgili yazılımdan silinmektedir.

Kullandığımız Ticari Paket Programlar, İnsan Kaynakları Programları, SQL veri tabanları gibi elektronik kayıt ortamlarına silme komutu verilerek verilerin silinmesi, merkezi sunucumuzda yer alan dosyalara veya dosyaların bulunduğu dizin üzerinde ilgili Kullanıcıların erişim haklarının kaldırılması; veri tabanlarında ilgili satırların veri tabanı komutları ile silinmesi veya taşınabilir medyada (USB, HDD, vb.) bulunan Kişisel Verilerin uygun yazılımlar kullanılarak silinmesi suretiyle veriler silinebilmektedir.

Ancak, bazı Kişisel Verilerin silinmesi sebebiyle diğer bir kısım verilere de sistemde erişimin mümkün olmadığı hallerde, silmeye konu Kişisel Veriler ilgili Veri Sahibi ile ilişkilendirilemeyecek duruma getirilerek arşivlenebilmektedir; bu durumda da ilgili Kişisel Veriler silinmiş sayılmaktadır. Böyle durumlarda Şirketimiz, Kişisel Verilere yalnızca yetkili kişiler tarafından erişilmesini sağlayacak şekilde gerekli her türlü teknik ve idari tedbiri almaktadır.

8.1.5. Kağıt Ortamında Bulunan Kişisel Verilerin Karartılması

Şirketimizin ticari faaliyetlerinin devamı için topladığı fiziki başvuru formları, sözleşmeler, özlük dosyaları gibi kağıt ortamında toplanan Kişisel Veriler, buldukları kağıt ortamında okunamayacak hale getirilerek de silinebilmektedir. Özellikle kötü niyetli, amaca yönelik olmayan kullanımı önlemek veya silinmesi talep edilen Kişisel Verileri silmek için, ilgili veya talebe konu tüm kişisel veriler fiziksel olarak belgenin bir kısmında kesilmekte veya geri döndürülemeyecek ve teknolojik çözümlerle okunamayacak şekilde sabit mürekkep kullanılarak görünemeyecek hale getirilmektedir.

However, in cases where, due to the deletion of some Personal data, it is impossible to access to some other data in the system, Personal Data so deleted may be archived by making them incapable of being associated with the related Data Owner; and in this case, relevant Personal data are deemed to have been deleted. In such cases, the COMPANY takes any and all necessary technical and administrative measures to enable only authorised people to have access to such Personal Data.

8.1.4. Deletion from Software Programmes Used

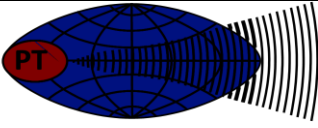
Personal Data stored in digital media in the COMPANY are deleted from any relevant software in a manner in which they will be inaccessible and unusable by any Related Users.

Data may be deleted by deleting the data by giving a deletion prompt to such electronic recording media as Commercial Package Programmes, Human Resources Programmes, SQL databases, etc. we use; by removing the Related Users' rights of access to the files contained in our central server or the directory where such files are available; by deleting any relevant lines available in databases using database prompts or by deleting any Personal data contained in portable media (USB, HDD, etc.) by using proper software.

However, in cases where, due to the deletion of some Personal data, it is impossible to access to some other data in the system, Personal Data so deleted may be archived by making them incapable of being associated with the related Data Owner; and in this case, relevant Personal data are deemed to have been deleted. In such cases, the COMPANY takes any and all necessary technical and administrative measures to enable only authorised people to have access to such Personal Data.

8.1.5. Blackout of Personal Data on Hardcopy

Personal data collected on such hardcopies as physical application forms, contracts, personal files, etc. for the continuation of its business activities by the COMPANY may also be deleted by making them illegible on the hardcopies they are contained. Particularly, in order to prevent any malicious use that is not to the purpose and to delete any Personal Data required to be deleted, all relevant or required personal data are physically cut off from a section of the document or made invisible by using indelible ink in a manner in which they will be irretrievable and not read by technological solutions.



PAGETEL Ltd. Şti.
İzmir- TÜRKİYE

KİŞİSEL VERİLERİN KORUNMASI VE İŞLENMESİ, KİŞİSEL VERİ SAKLAMA VE İMHA POLİTİKASI

Protection, Processing Storage and Destruction of Personal Data Policy
Kod/Code # FR-03.40

Tarih / Date :

Sayfa / Page : 50 /
54

8.1.6. Bulut Sisteminden Silme

Şirket bünyesinde bulut sistemlerinde muhafaza edilen/saklanan Kişisel Veriler, İlgili Kullanıcılar için hiçbir şekilde erişilemez ve tekrar kullanılamaz hale getirilecek biçimde bulut sisteminden kalıcı olarak silinmektedir.

Ancak, bazı Kişisel Verilerin silinmesi sebebiyle diğer bir kısım verilere de sistemde erişimin mümkün olmadığı hallerde, silmeye konu Kişisel Veriler ilgili Veri Sahibi ile ilişkilendirilemeyecek duruma getirilerek arşivlenebilmektedir; bu durumda da ilgili Kişisel Veriler silinmiş sayılmaktadır. Böyle durumlarda Şirketimiz, Kişisel Verilere yalnızca yetkili kişiler tarafından erişilmesini sağlayacak şekilde gerekli her türlü teknik ve idari tedbiri almaktadır.

9. KİŞİSEL VERİ SAHİPLERİNİN HAKLARI; BU HAKLARIN KULLANILMASI VE DEĞERLENDİRİLMESİ METODOLOJİSİ

9.1. Veri Sahibinin Hakları ve Bu Haklarını Kullanması

9.1.1. Kişisel Veri Sahibinin Hakları

Kişisel veri sahipleri aşağıda yer alan haklara sahiptirler:

- Kişisel veri işlenip işlenmediğini öğrenme,
- Kişisel verileri işlenmişse buna ilişkin bilgi talep etme,
- Kişisel verilerin işlenme amacını ve bunların amacına uygun kullanılıp kullanılmadığını öğrenme,
- Yurt içinde veya yurt dışında kişisel verilerin aktarıldığı üçüncü kişileri bilme,
- Kişisel verilerin eksik veya yanlış işlenmiş olması hâlinde bunların düzeltilmesini isteme ve bu kapsamda yapılan işlemin kişisel verilerin aktarıldığı üçüncü kişilere bildirilmesini isteme,
- KVK Kanunu ve ilgili diğer kanun hükümlerine uygun olarak işlenmiş olmasına rağmen, işlenmesini gerektiren sebeplerin ortadan kalkması hâlinde kişisel verilerin silinmesini veya yok edilmesini isteme ve bu kapsamda yapılan işlemin kişisel verilerin aktarıldığı üçüncü kişilere bildirilmesini isteme,
- İşlenen verilerin münhasıran otomatik sistemler vasıtasıyla analiz edilmesi suretiyle kişinin kendisi aleyhine bir sonucun ortaya çıkmasına itiraz etme,
- Kişisel verilerin kanuna aykırı olarak işlenmesi sebebiyle zarara uğraması hâlinde zararın giderilmesini talep etme.

8.1.6. Deletion from the Cloud System

Personal data maintained/stored in the Cloud systems in the COMPANY are permanently deleted from the Cloud system in a manner in which they will be made in accessible and reusable by the Related Users.

However, in cases where, due to the deletion of some Personal data, it is impossible to access to some other data in the system, Personal Data so deleted may be archived by making them incapable of being associated with the related Data Owner; and in this case, relevant Personal data are deemed to have been deleted. In such cases, the COMPANY takes any and all necessary technical and administrative measures to enable only authorised people to have access to such Personal Data.

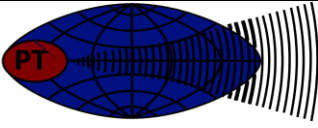
9. RIGHTS OF THE OWNERS OF PERSONAL DATA; METHODOLOGY FOR THE EXERCISE AND EVALUATION OF SUCH RIGHTS

9.1. Rights of the Data Owner and Exercise of Such Rights

9.1.1. Rights of the Personal Data Owner

Personal data Owners have the following rights:

- to learn whether or not their personal data are processed;
- if their personal data have been processed, to request information thereon;
- to learn the purpose of processing their personal data and whether or not such data are used to the purpose;
- to know any third parties to whom their personal data are transferred at home and abroad;
- in case their personal data have been deficiently or erroneously processed, to require the same to be corrected and to request that the action taken to that effect is to be notified to the third parties to whom such data have been transferred;
- in case the reasons for the processing of their personal data cease to exist –even though they have been processed pursuant to the PPD Act and any other relevant legal provisions, to require their personal data to be deleted or destroyed and to request the action taken to that effect to be notified to the third parties to whom such data have been transferred;
- to raise objection to the emergence of any outcome against the person himself/herself by solely analysing the processed data via automated systems;
- in case they incur losses due to illegal processing of their personal data, to require their losses to be compensated



PAGETEL Ltd. Şti.
İzmir- TÜRKİYE

KİŞİSEL VERİLERİN KORUNMASI VE İŞLENMESİ, KİŞİSEL VERİ SAKLAMA VE İMHA POLİTİKASI

Protection, Processing Storage and Destruction of Personal Data Policy
Kod/Code # FR-03.40

Tarih / Date :

Sayfa / Page : 51 /
54

9.1.2. Kişisel Veri Sahibinin Haklarını İleri Süremeyeceği Haller

Kişisel veri sahipleri, KVK Kanunu'nun 28. maddesi gereğince aşağıdaki haller KVK Kanunu kapsamı dışında tutulduğundan, kişisel veri sahiplerinin bu konularda 10.1.1.'de sayılan haklarını ileri süremezler:

- Kişisel verilerin resmi istatistik ile anonim hâle getirilmek suretiyle araştırma, planlama ve istatistik gibi amaçlarla işlenmesi.
- 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.
- 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.
- Kişisel verilerin soruşturma, kovuşturma, yargılama veya infaz işlemlerine ilişkin olarak yargı makamları veya infaz mercileri tarafından işlenmesi.

KVK Kanunu'nun 28/2 maddesi gereğince; aşağıda sıralanan hallerde kişisel veri sahipleri zararın giderilmesini talep etme hakkı hariç, 10.1.1.'de sayılan diğer haklarını ileri süremezler:

- Kişisel veri işleminin suç işlenmesinin önlenmesi veya suç soruşturması için gerekli olması.
- Kişisel veri sahibi tarafından kendisi tarafından alenileştirilmiş kişisel verilerin işlenmesi.
- Kişisel veri işleminin kanunun verdiği yetkiye dayanarak 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.
- Kişisel veri işleminin bütçe, vergi ve mali konulara ilişkin olarak Devletin ekonomik ve mali çıkarlarının korunması için gerekli olması.

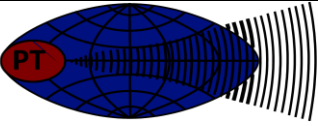
9.1.2. Cases in Which Personal Data Owner May Not Claim His/Her Rights

Personal data owners may not claim their rights on the following matters listed in the subparagraph 10.1.1 as such rights are excluded from the PPD Act as per the article 28 of the PPD Act:

- processing of personal data for such purposes as research, planning and statistics by anonymizing the same through official statistics;
- processing of personal data for such purposes as arts, history, literature or science or within the scope of freedom of speech provided that it would not violate national defence, national security, public security, public order, economic security, privacy of life or personal rights or that it would not constitute a crime;
- processing of personal data within the scope of preventive, protective and informative activities implemented by any public organisations and institutions assigned and authorised by law in order to insure national defence, national security, public security, public order or economic security;
- processing of personal data in connection with investigation, prosecution, adjudication and enforcement activities by judicial or enforcement authorities.

As per the second paragraph of the article 28 of the PPD Act, personal data owners may not claim their rights as listed in subparagraph 10.1.1 other than their right to require the compensation of their loss in the following cases:

- that processing of personal data is necessary for the prevention of the commitment of a crime or for a criminal investigation;
- processing of personal data anonymized by the personal data owner himself/ herself;
- that processing of personal data is necessary for the performance of inspectional or regulatory assignments and disciplinary investigations or prosecutions by the assigned and authorised public organisations and institutions as well as by the professional organisations of public organisation nature on the basis of the authorisation granted by law;
- that processing of personal data is necessary for the economic and financial interests of the State in connection with budgetary, taxation and financial issues.



PAGETEL Ltd. Şti.
İzmir- TÜRKİYE

KİŞİSEL VERİLERİN KORUNMASI VE İŞLENMESİ, KİŞİSEL VERİ SAKLAMA VE İMHA POLİTİKASI

Protection, Processing Storage and Destruction of Personal Data Policy
Kod/Code # FR-03.40

Tarih / Date :

Sayfa / Page : 52 /
54

9.1.3. Kişisel Veri Sahibinin Haklarını Kullanması

Kişisel Veri Sahipleri bu bölümün 9.1.1. Başlığı altında sıralanan haklarına ilişkin taleplerini kimliklerini tespit edecek bilgi ve belgelerle ve aşağıda belirtilen yöntemlerle veya Kişisel Verileri Koruma Kurulu'nun belirlediği diğer yöntemlerle Başvuru Formu'nu doldurup imzalayarak Şirkete ücretsiz olarak iletebileceklerdir:

- www.pagetel.com.tr adresinde bulunan formun doldurulduktan sonra ıslak imzalı bir nüshasının bizzat elden veya noter aracılığı ile Çamlık Cad. No:44 35414 - Gaziemir, İzmir/Türkiye adresine iletilmesi
- www.pagetel.com.tr adresinde bulunan formun doldurulup 5070 Sayılı Elektronik İmza Kanunu kapsamındaki "güvenli elektronik imza"nızla imzalandıktan sonra güvenli elektronik imzalı formun pagetel@hs01.kep.tr adresine kayıtlı elektronik posta ile gönderilmesi

Kişisel veri sahipleri adına üçüncü kişilerin başvuru talebinde bulunabilmesi için veri sahibi tarafından başvuruda bulunacak kişi adına noter kanalıyla düzenlenmiş özel vekâletname bulunmalıdır.

9.1.4. Kişisel Veri Sahibinin KVK Kurulu'na Şikâyetle Bulunma Hakkı

Kişisel veri sahibi KVK Kanunu'nun 14. maddesi gereğince başvurunun reddedilmesi, verilen cevabın yetersiz bulunması veya süresinde başvuruya cevap verilmemesi hâllerinde; Şirketin cevabını öğrendiği tarihten itibaren otuz ve herhâlde başvuru tarihinden itibaren altmış gün içinde KVK Kurulu'na şikâyetle bulunabilir.

9.2. Şirketin Başvurulara Cevap Vermesi

9.2.1. Şirketin Başvurulara Cevap Verme Usulü ve Süresi

Kişisel veri sahibinin, bu bölümün 9.1.3. başlıklı kısmında yer alan usule uygun olarak talebini Şirkete iletmesi durumunda Şirket talebin niteliğine göre en geç otuz gün içinde ilgili talebi ücretsiz olarak sonuçlandıracaktır. Ancak, KVK Kurulunca bir ücret öngörülmesi hâlinde, Şirket tarafından başvuru sahibinden KVK Kurulunca belirlenen tarifedeki ücret alınacaktır.

9.1.3. Exercise of His/Her Rights by Personal Data Owner

Personal Data Owners will deliver their requests for their rights as listed in the subparagraph 9.1.1 of this present section to the COMPANY on free of charge basis in the accompaniment of any information and documents which will identify them and by the following methods by completing and signing the Application Form or by any other methods to be identified by the Protection of Personal Data Committee:

- that the form available at www.pagetel.com.tr is to be completed and a copy thereof bearing an original signature be delivered to Çamlık Cad. No:44 35414 - Gaziemir, İzmir/Turkey personally or through a notary public;
- that the form available at www.pagetel.com.tr is to be completed and signed with "safe electronic signature" as per the Electronic Signature Act No. 5070 and that the form bearing the safe electronic signature be sent to pagetel@hs01.kep.tr via registered electronic mail.

There must be a special power of attorney drawn up by a notary public in the name of the person who will file an application on behalf of the personal data owner so that any third parties may file an application on behalf of personal data owners.

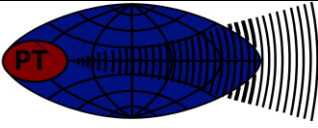
9.1.4. Personal Data Owner's Right to File a Complaint with the PPD Committee

Personal data owner may file a complaint with the PPD Committee not later than thirty days following the date when he/she learns the COMPANY's reply but at all events not later than sixty days following the date of application in case his/her application is rejected, if the reply given remains insufficient or if the application is not replied in due time as per the articles 14 of the PPD Act.

9.2. COMPANY's Reply to Applications

9.2.1. Method and Period for the COMPANY to Reply Applications

In case the personal data owner delivers his/her request to the COMPANY in compliance with the method as set forth in the subparagraph 9.1.1 of this present section, the COMPANY will conclude the relevant request on free of charge basis not later than thirty days by the nature of the request. However, in case it is prescribed by the PPD Committee, the COMPANY will charge the fee as contained in the price list determined by the PPD Committee from the applicant.



PAGETEL Ltd. Şti.
İzmir- TÜRKİYE

KİŞİSEL VERİLERİN KORUNMASI VE İŞLENMESİ, KİŞİSEL VERİ SAKLAMA VE İMHA POLİTİKASI

Protection, Processing Storage and Destruction of Personal Data Policy
Kod/Code # FR-03.40

Tarih / Date :

Sayfa / Page : 53 /
54

9.2.2. Şirketin Başvuruda Bulunan Kişisel Veri Sahibinden Talep Edebileceği Bilgiler

Şirket, başvuruda bulunan kişinin kişisel veri sahibi olup olmadığını tespit etmek adına ilgili kişiden bilgi talep edebilir. Şirket, kişisel veri sahibinin başvurusunda yer alan hususları netleştirmek adına, kişisel veri sahibine başvurusu ile ilgili soru yöneltebilir.

9.2.3. Şirketin Kişisel Veri Sahibinin Başvurusunu Reddetme Hakkı

Şirket aşağıda yer alan hallerde başvuruda bulunan kişinin başvurusunu, gerekçesini açıklayarak reddedebilir:

- Kişisel verilerin resmi istatistik ile anonim hâle getirilmek suretiyle araştırma, planlama ve istatistik gibi amaçlarla işlenmesi.
- 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.
- 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.
- Kişisel verilerin soruşturma, kovuşturma, yargılama veya infaz işlemlerine ilişkin olarak yargı makamları veya infaz mercileri tarafından işlenmesi.
- Kişisel veri işleminin suç işlenmesinin önlenmesi veya suç soruşturması için gerekli olması.
- Kişisel veri sahibi tarafından kendisi tarafından alenileştirilmiş kişisel verilerin işlenmesi.
- Kişisel veri işleminin kanunun verdiği yetkiye dayanılarak görevli ve yetkili kamu kurum ve kuruluşları ile kamu kurumu niteliğindeki meslek kuruluşlarının, denetleme veya düzenleme görevlerinin yürütülmesi ile disiplin soruşturma veya kovuşturması için gerekli olması.
- Kişisel veri işleminin bütçe, vergi ve mali konulara ilişkin olarak Devletin ekonomik ve mali çıkarlarının korunması için gerekli olması.
- Kişisel veri sahibinin talebinin diğer kişilerin hak ve özgürlüklerini engelleme ihtimali olması
- Orantısız çaba gerektiren taleplerde bulunulmuş olması.

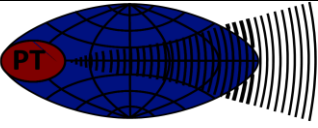
9.2.2. Information Which the COMPANY May Require from the Applying Personal Data Owner

The COMPANY may require information from the related person in order to find out whether or not the applicant is a personal data owner. The COMPANY may direct questions to the personal data owner in order to clarify the issues as contained in the application filed by the personal data owner.

9.2.3. COMPANY's Right to Reject the Personal Data Owner's Application

The COMPANY may reject the application filed by the applicant by disclosing its reasons in the following cases:

- processing of personal data for such purposes as research, planning and statistics by anonymizing the same through official statistics;
- processing of personal data for such purposes as arts, history, literature or science or within the scope of freedom of speech provided that it would not violate national defence, national security, public security, public order, economic security, privacy of life or personal rights or that it would not constitute a crime;
- processing of personal data within the scope of preventive, protective and informative activities implemented by any public organisations and institutions assigned and authorised by law in order to insure national defence, national security, public security, public order or economic security;
- processing of personal data in connection with investigation, prosecution, adjudication and enforcement activities by judicial or enforcement authorities;
- that processing of personal data is necessary for the prevention of the commitment of a crime or for a criminal investigation;
- processing of personal data anonymized by the personal data owner himself/ herself;
- that processing of personal data is necessary for the performance of inspectional or regulatory assignments and disciplinary investigations or prosecutions by the assigned and authorised public organisations and institutions as well as by the professional organisations of public organisation nature on the basis of the authorisation granted by law;
- that processing of personal data is necessary for the economic and financial interests of the State in connection with budgetary, taxation and financial issues;
- that the personal data owner's request may possibly impede other people's rights and freedoms;



PAGETEL Ltd. Şti.
İzmir- TÜRKİYE

KİŞİSEL VERİLERİN KORUNMASI VE İŞLENMESİ, KİŞİSEL VERİ SAKLAMA VE İMHA POLİTİKASI

Protection, Processing Storage and Destruction of Personal Data Policy
Kod/Code # FR-03.40

Tarih / Date :

Sayfa / Page : 54 / 54

10. ŞİRKET KİŞİSEL VERİLERİN KORUNMASI VE İŞLENMESİ POLİTİKASI'NIN DİĞER POLİTİKALARLA OLAN İLİŞKİSİ

Şirket, işbu Politika ile ortaya koymuş olduğu esasların ilişkili olduğu kişisel verilerin korunması ve işlenmesi konusunda iç kullanıma yönelik alt politikalar da oluşturabileceği gibi çalışanlar başta olmak üzere belli kişi gruplarına yönelik olarak ayrıca başka politikalar da oluşturmaktadır.

Şirket içi politikalarının esasları, ilgili olduğu ölçüde kamuoyuna açık politikalara yansıtılarak, ilgililerinin bu çerçevede bilgilenmesi ve Şirketin yürütmekte olduğu kişisel veri işleme faaliyetleri hakkında şeffaflık ve hesap verilebilirliğin sağlanması hedeflenmiştir.

10. RELATIONSHIP OF THE COMPANY'S POLICY FOR THE PROTECTION AND PROCESSING OF PERSONAL DATA WITH OTHER POLICIES

While the COMPANY may establish sub-policies for internal use on the protection and processing of personal data with which the principles which the COMPANY has set forth by this Policy, it also establishes other policies intended for certain groups of people including but not limited to employees.

Principles of the in-house policies are represented in the public policies to the extent they are relevant, thus aiming at allowing any interested parties to be informed in this context and ensuring transparency and accountability about the personal data processing activities carried out by the COMPANY.