Business-Non Contain Personal Data

PROTECTION OF PERSONAL DATA AND PRIVACY STATEMENT

As DP World, we attach importance to the privacy and security of your personal data. In this context, we would like to inform you about how we process personal data belonging to our customers, suppliers, business partners, their employees and officials and all other third parties while conducting our business relations, for what purposes we use it and how we protect this information.

All concepts and expressions used in this notification shall express the meaning attributed to them in the Personal Data Protection Law No.6698 ("PDPL") and other legislation. The term "you" in this Notice refers to your person. The term personal data is used to include special quality personal data. The meanings expressed by the terms and abbreviations in the policy are included in the ANNEX - Abbreviations section.

We would like to remind you that if you do not accept the notification, you should not forward your personal data to us. If you choose not to provide us with your personal data, in some cases we will not be able to provide you with our services, respond to your requests, or ensure the full functionality of our services.

We would like to remind you that it is your responsibility to ensure that the personal data you submit to our company are accurate, complete and up to date as far as you know. Beyond that, if you share other people's data with us, it will be your responsibility to collect such data in accordance with local legal requirements. In this case, it will mean that you have obtained all necessary permissions from the third party to collect, process, use and disclose their information, and our Company will not be held responsible in this context.

ABOUT DP WORLD

DP World is the world's fourth container terminal operator with over 45,000 professional employees operating 78 terminals in 40 countries. Low carbon emissions and supply chain equipped with environmentally friendly technology aimed at the efficiency, the first truck parking space in Turkey's port area, 550 Million Dollars of the investment costs on DP World Yarımca Container port, a centralized activity planning with the latest technology terminal operating, gate automation and equipment management systems. DP World Yarımca Container Terminal has a world-class organization with its expert, dynamic and innovative team that derives its service quality and competitive power from the richness created by different cultures.

The statement "we" or the "Company" or "DP World" statements, Mimar Sinan neighborhood Mehmet Akif Ersoy street No: 168, 41780 Yarımca Gulf- Turkey operating at Istanbul Trade Registry before the 3747 Central Registration System No registered with DP World Yarımca Port Management Incorporated Company (“DP World”), regarding the personal data processing activities carried out as a Data Controller

PERSONAL DATA PROCESSING PRINCIPLES

All personal data processed by our company are processed in accordance with PDPL and relevant legislation. The basic principles and principles that we pay attention to while processing your personal data in accordance with Article 4 of PDPL are explained below:

• Processing in Compliance with the Law and the Rules of Good Faith: Our Company; acts in accordance with the principles introduced by legal regulations and the general rule of trust and honesty in the processing of personal data. In this context, our Company takes into account the proportionality requirements in the processing of personal data, and does not use personal data outside of the purpose.

• Keeping Personal Data Accurate and Updated When Required: Our Company; It ensures that the personal data it processes is accurate and up to date, taking into account the fundamental rights of personal data owners and their own legitimate interests.

• Processing for Specific, Clear and Legitimate Purposes: Our company clearly and precisely determines the purpose of processing personal data that is legitimate and legal. Our company processes personal data in connection with the products and services it offers and as much as necessary for them.

• Being Related, Limited and Measured for the Purpose of Processing: Our company processes personal data in a way that is convenient for the realization of the specified purposes and avoids the processing of personal data that is not related to the realization of the purpose or is not needed.

• Preserving for the Period Stipulated in the Relevant Legislation or Required for the Purpose of Processing:

Our company keeps personal data only for the period specified in the relevant legislation or for the purpose for which they are processed. In this context, our Company first determines whether a period is stipulated for the storage of personal data in the relevant legislation, if a period is specified, it acts in accordance with this period, if a period is not specified, it stores the personal data for the period required for the purpose for which they are processed. Personal data are deleted, destroyed or anonymized by our Company in the event of the expiration of the period or the disappearance of the reasons for processing.

DATA OWNER CATEGORIES

The categories of data owners, except for employees whose personal data are processed by our company (including interns and sub-employer company employees), are shown in the table below. A separate policy regarding the processing of personal data of our employees has been established and implemented within the company. Persons who fall outside of the following categories can also direct their requests to our Company within the scope of PDPL; The demands of these people will also be

RELATED PERSON CATEGORY	**DESCRIPTION**
Costumer	Real or legal persons purchasing our services
Potential Customer	Real or legal persons who have requested or been interested in using our services or who have been evaluated in accordance with the rules of customary and honesty that they may have this interest in.
Visitor	Real persons who enter the physical facilities (offices etc.) owned or organized by our company for various purposes or visit our websites
Third Person	Third party natural persons (e.g. surety, companion, family members and relatives) who are associated with our Company in order to ensure the security of commercial

	transactions between our Company and the above-mentioned parties or to protect the rights of the aforementioned persons and to obtain benefits, or personal data of our Company, even if not explicitly stated in the Policy all natural persons (e.g. former employees) that they have to operate for a specific purpose
Employee Candidate / Trainee Candidate	Real persons who have applied for a job to our company in any way or who have opened their curriculum vitae and related information to our Company
Group Company Employee	Employees and representatives of DP World group companies abroad of which our company is a member.
Employees and Shareholders of Institutions We Cooperate With	Real persons, whose officials work in the institutions with which our Company has any business relationship (business partners, suppliers, etc. but not limited to these), including the shareholders and officials of these institutions

WHEN DO WE COLLECT PERSONAL DATA ABOUT YOU?

We collect your personal data mainly in the following situations:

1) When you purchase or use our services,

2) When you sell goods or provide services to us,

3) When you subscribe to our newsletters, choose to receive our marketing messages,

4) When you contact us by complaint or feedback via our website, e-mail, social media platforms, other online channels or by phone,

5) When you apply for a job with our company,

6) When you attend our company events, seminars, conferences and organizations,

7)Indirectly, for example, by using "cookies" and customizing the software used to tailor the website to your particular preferences, or monitoring your use of certain pages of the site (for example, your IP address) or other technical methods that enable us to monitor your use of the site.

8) When you contact us for any purpose as a potential customer / supplier ,business partner , sub-employer,

We will only process the personal data we obtain in the above cases in accordance with this Statement.

WHAT PERSONAL DATA DO WE PROCESS ABOUT YOU?

The personal data we process about you vary according to the type of business relationship between us (ex. customer, supplier, business partner, etc.) and the method of communicating with us (telephone, e-mail, website, printed documents, etc.).

Basically, our personal data processing methods, through our website, by phone or e-mail, through electronic applications specific to our customers, where you participate in our business events, competitions, promotions and surveys, filling in documents arising from our feedback and similar

legislative obligations, or in any other way are situations. In this context, the personal data we process about you are described under the following categories:

Data categories	Examples
ID information:	Information on identity documents such as name, surname, title, date of birth
Contact information:	Email, phone number, address
Account login information:	Login ID, password, and other security codes
Special quality personal data :	Health data we need to receive in accordance with the legislation
Pictures and / or videos that	photo and video images and audio data processed when you visit our company for security
can identify you and	reasons or when you attend events organized by our company, visual data processed with
in-port location data :	CCTV records when you visit our company facilities, in port location data.

DATA CATEGORIES	EXAMPLES
Financial Data :	Bank account data, invoice information, company credit card data issued on behalf of staff
Any other information you decide to voluntarily share with DP World:	Feedback, opinions, requests and complaints, evaluations, comments and evaluations regarding these, uploaded files, interests, detailed review process before establishing a business relationship with you, through personal data you share with your own initiative, social media, online platforms or other media. Information provided for
Electronic data collected automatically	When you visit or use our website or our apps, subscribe to our newsletters, interact with us through other electronic channels, in addition to the information you directly transmit to us, we also collect electronic data sent to us by your computer, mobile phone or other access device (e.g. device hardware model, IP address, operating system version and settings, time and time of using our digital channel, your actual location that can be collected when you enable location-based features, links you click, motion sensor data, etc.) Your personal data, audit and inspection data processed within the scope of the determination, follow-up of our legal receivables and rights and the performance of our debts and compliance with our legal obligations and our Company's policies
Legal action and compliance information	As a result of the operations carried out by our business units within the framework of our services, the information obtained and produced about the data owner supplier or the employee within the customer supplier, such as the signature authority
Incident management and	Information and evaluations collected about events that have the potential to affect our company's employees, directors or shareholders, vehicle license plate and vehicle

security information:	information, transportation and travel information, the type of near-miss incident related to damaged containers / goods / ships in the port, expertise report.
Corporate customer / supplier data:	To the extent permitted by applicable laws and regulations, we also collect your personal data through public databases, social media platforms, and the methods and platforms that our business partners we work with collect personal data on our behalf. For
Personal data collected from other sources:	example, before establishing a business relationship with you, we conduct research on you from public sources to ensure the technical, administrative and legal security of our business activities and transactions. In addition, it may be possible for you to transmit some personal data belonging to third parties to us (For example, personal data of guarantor, companion, family members, etc.). In order to manage our technical and administrative risks, we process your personal data through methods used in these areas in accordance with the generally accepted legal, commercial practice and good faith. In addition, telephone, website, etc. We record the personal data you transmit to us on your own initiative through the platforms and process them for the resolution of your requests and Problems.

PROCESSING PERSONAL DATA OF EMPLOYEE CANDIDATES

In addition to the above personal data categories of the Employee Candidates, we understand the candidate's experience and qualifications and evaluate their suitability for the vacant position, check the accuracy of the information transmitted if necessary, and conduct research about the candidate by contacting the third parties whose contact information is given, In order to communicate with the candidate, to recruit suitable for the vacant position, to comply with legal regulations and to apply our Company's recruitment rules and human resources policies, the school he graduated, his previous work experience, disability, etc. we collect your personal data.

Personal data of employee candidates, job application form available in written and electronic media, our company's electronic job application platform, applications sent to our company physically or by e-mail, employment and consultancy companies, face-to-face or electronic interviews, The checks made by the employee candidate are processed by the recruitment tests performed by human resources experts to evaluate the candidate's suitability during the recruitment process.

Employee candidates are informed in detail in accordance with PDPL with a separate document before submitting their personal data while applying for a job, and their explicit consent is obtained for the necessary personal data processing activities.

OUR POLICY ON COOKIES

For more information about how we use cookies and other tracking technologies ..... Please read our Cookie Policy. Generally, a "cookie" is the name given to the information sent and stored on the user's computer by an Internet service server. ‘The information contained in the cookies can be used when the user returns to the website in question. ‘Cookies contain various information, including how many times the user entered the site in question. By using individual session cookies for each user, we can monitor how you use the site during a single session. ‘Thanks to cookies, we determine which browser you are using and offer you some special services.

Information stored in cookies includes the date of visit, the time of visit, the pages viewed, the time spent in the Online Transactions Center, and the sites visited just before or after the visit to the Online Transactions Center. By evaluating the data collected through these cookies used during your visit to the Online Operations Center, you can then display advertisements for products that you may be potentially interested in during your visit to other websites. It is possible to block cookies via your internet browser.

By using the "help" function available in most browsers, you can learn how to prevent your computer from receiving al cookies ', find out if ip cookies' are sent, and disable them completely. However, we would like to remind you that if you disable cookies, you may not be able to use this site fully.

This site uses cookies 'for a variety of purposes, including:

• Access certain information after entering the site in order to provide you with personalized content;

• Track your preferences when using this site, such as your preferred date and number formats. We value the privacy of your information. We apply the following rules to protect the privacy and security of your confidential information to the highest possible level:

• This site does not always keep "cookies" on your disk drive. Cookies are removed when you close your browser or leave the site.

• Information in all cookies 'sent to your computer from this site are sent encrypted.

PROCESSING PERSONAL DATA OF OUR VISITORS AT OUR OFFICES AND THE PORT REGION

Our company processes your personal data for the purpose of ensuring the physical security of our Company, our employees and visitors and controlling the workplace rules during the entrance and exit procedures of visitors to its buildings and port area.

The visitor is informed about the processing of personal data with an illumination text in the security entrance before the information is received. In this context, as our company has a legitimate interest, PDPL. In accordance with 5/2 / f, the visitor's explicit consent is not taken. These data are physically kept in the visitor logbook and in the digital environment and are not transferred to another medium unless there is a situation that threatens the security of the Company. However, this information can be used in cases such as crime prevention and Company security.

In addition, for the purposes specified in the Policy and providing security by our Company; During your stay in our company's offices, internet access is available to our visitors who request. In this case, the log records regarding your internet access are recorded in accordance with the Law No. 5651 and the mandatory provisions of the legislation regulated according to this law; These records are only processed when requested by the authorized public institutions and organizations or in order to fulfill our legal obligation in the audit processes to be carried out within the Company.

Only a limited number of DP World employees can access the log records obtained within this framework. Company employees, who have access to the aforementioned records, access these records

only for use in the request or audit processes from the authorized public institutions and organizations and share them with legally authorized persons.

PROCESSING PERSONAL DATA THROUGH CLOSED CIRCUIT CAMERA RECORDING

Security cameras are used to ensure the security of our company and our facilities and personal data is processed in this way. Our company, within the scope of security camera surveillance activity; It aims to increase the quality of the service provided, to ensure the safety of life and property of the physical premises of the company and the persons within the company, to prevent abuse, to protect the legitimate interests of data owners.

Personal data processing activities performed by our company with security cameras are carried out in accordance with the Constitution, PDPL, Law No. 5188 on Private Security Services and the relevant legislation.

Our company, PDPL. 4, processes personal data in a limited and measured manner in connection with the purpose for which they are processed. It is not subjected to monitoring the privacy of the person in a way that may result in intervention that exceeds security objectives. In this context, warning signs are placed in common areas where CCTV recording is made and data owners are informed. Since our company has a legitimate interest in keeping CCTV records, express consent is not taken. In addition, PDPL. In accordance with 12th, necessary technical and administrative measures are taken to ensure the security of personal data obtained as a result of CCTV monitoring.

In addition, a procedure has been prepared regarding the areas with CCTV cameras, the monitoring areas of the cameras, and the recording time, and implementation has been implemented in our company. This procedure is taken into consideration before the CCTV camera is installed and the camera is placed later. It is not allowed to place cameras beyond the security purpose and beyond the privacy of the persons. Only a certain number of Company personnel access CCTV camera images and these authorizations are regularly reviewed. Personnel who have access to these records sign a commitment to protect personal data in accordance with the law.

By means of a total of 144 security cameras located in the service area of the building exterior, dining hall, visitor entrances, parking lot, security cabin and floor corridors, which are the areas where security is established and monitored in accordance with the ISPS Code, and the entrance gates of our company offices and the port area and the port areas where operations are carried out. In order to ensure building security, footage is recorded and the registration process is supervised by DP World Yarımca Security Unit.

FOR WHICH PURPOSES DO WE USE YOUR PERSONAL DATA?

Our purposes for using your personal data vary depending on the type of business relationship between us (customer, supplier, business partner, etc.). Basically, our purposes for processing your personal data are as follows. Personal data processing activities related to Employee Candidates are explained under the "Processing of Personal Data of Employee Candidates" section above.

Business-Non Contain Personal Data

Our Purposes of Processing Personal Data	**Examples**
Evaluating potential suppliers / business partners	Conducting our review and conflict of interest process in accordance with our risk rules
Direct Marketing	Marketing notices regarding our services by email and telephone
Customer Establishment and management of relations, execution and conclusion of the contract process with our suppliers and business partners	Performing sales transactions of the services offered by our company, submitting offers for our services, invoicing, establishing and executing contracts, ensuring post-contract legal transaction security, managing logistics processes, developing products and services, evaluating new technologies and applications, and determining and implementing our company's commercial and business strategies , operations management (request, offer, evaluation, order, budgeting, contract), investment quality processes and operations, internal system and application management operations, financial operations, financial affairs management, procurement of goods and services, managing the registration process for our website applications, commercial to offer alternatives to legal or real people with whom they are in contact

OUR PURPOSES OF PROCCESING PERSONAL DATA	EXAMPLES
Execution of processes	To make marketing notifications about our services via e-mail and telephone, to conduct satisfaction surveys or to evaluate your opinions, complaints and comments you have made through social media, online platforms or other media, to inform our customers about company innovations, campaigns and promotions, advertising, promotion , carrying out marketing activities, congresses, seminars, etc. organizing events.
Contact and support on your request	Execution of tax and insurance processes, fulfillment of our legal obligations arising from the relevant legislation, especially the Law No.5651 and other legislation, the Turkish Penal Law No.5237 and the Personal Data Protection Law No.6698 and customs legislation, carrying out the processes before official institutions, preparing a capacity report, Fulfillment of obligations such as obtaining environmental permit, record keeping and information obligations, compliance and auditing, audits and inspections of official authorities, follow-up and conclusion of our legal rights and lawsuits, carrying out the necessary processes within the scope of compliance with the laws and regulations we are subject to, Obtaining customs permits for persons who will enter the customs area within the scope of the customs legislation, within the scope of the requirements and obligations determined to ensure the fulfillment of the legal obligations specified in the PDPL as required or required.
	Carrying out the necessary audit activities to protect the interests and interests of the company, conducting conflict of interest controls, ensuring the legal and commercial security of the persons in business relations with our company, keeping CCTV records for the protection of company devices and assets, taking technical and administrative security measures, and improving the services we offer. implementation and supervision of workplace rules, management of quality

Protection of company interests and ensuring their security	processes, planning and execution of social responsibility activities, protecting the commercial reputation and trust established by DP World group companies, all incidents, accidents, complaints, lost stolen etc. To make the necessary interventions and to take precautions by reporting the situations, to transfer the rules to be followed for dangerous situations that may occur during maintenance and repair, and to measure the professional competence of subcontractors, to ensure the order of the employees of the company and to obtain the necessary information in terms of security, to carry out the necessary quality and standard audits, or Fulfilling our reporting and other obligations determined by laws and regulations, managing insurance and damage processes related to the damaged customer containers good hips in the port with brokers and insurance companies
Planning and execution of company commercial activities	In line with the purpose of determining, planning and implementing the commercial policies of the company in the short, medium and long term, determining and implementing commercial and business strategies; Communication conducted by our company, conducting market research or getting finished.
Reporting and audit	Providing communication with DP World group companies abroad, carrying out necessary activities, internal audit and reporting processes.

HOW DO WE USE YOUR PERSONAL DATA FOR MARKETING?

As a rule, we obtain your consent to process your personal data. Our company may send you regular promotional communications about its services, events and promotions. Such promotional communications may be sent to you via different channels such as email, phone, SMS text messages, mail and third party social networks.

In order to provide you with the best personalized experience, sometimes these communications may be adapted to your preferences (for example, based on the results we derive from your website visits, or based on links you click in our emails, as you tell us about them).

Based on your consent, processing for the purpose of offering you special products and services such as opportunity and product / service advertisements, using Cookies for this purpose, providing you with special advertisements, campaigns, advantages and other benefits for sales and marketing activities, and carrying out other marketing and CRM activities. sending of electronic commercial messages (such as campaigns, newsletters, customer satisfaction surveys, product and service advertisements) for the purpose of processing, creating new product and service models; sending gifts and promotions; We may carry out marketing activities in order to organize corporate communication and other events and invitations in this context and to provide information about them.

When required by the applicable legislation, we will ask for your consent before starting the above activities. You will also be given the opportunity to withdraw stop your consent at any time. In particular, you can always stop marketing-related notifications from being sent to you by following the unsubscribe instructions included in each e-mail and SMS message.

If you sign in to a DP World account, you may be given the option to change your communication preferences under the relevant section of our website or app. You can always contact us to stop sending

marketing communications (contact details can be found in the section "What Are Your Rights Regarding Your Personal Data? Below).

Within the scope of our digital media activities, we organize campaigns and competitions on social media platforms from time to time. In this context, your name and surname information, contact information (phone number and address), visual and audio data such as photographs and videos, personal comments are processed for the purpose of identifying the winning competitors, sending gifts, and providing necessary organizations with the cargo company. Since you transmit your personal data to us in accordance with PDPL article 5/2 we do not seek your explicit consent.

WHAT LEGAL REASONS DO WE PROCESS YOUR PERSONAL DATA?

Your personal data, especially the Turkish Commercial Code No. 6102, the Turkish Code of Obligations No. 6098, the Tax Procedure Law No. 213, electronic commerce legislation.

Legal Reason	EXAMPLES
In cases where we need your explicit consent in accordance with PDPL and other legislation, we process based on your consent (In this case, we would like to remind you that you can withdraw your consent at any time)	We obtain your consent to carry out our marketing activities.
In any situation permitted by applicable legislation	Tax Procedure Law m. Including the name of the relevant person on the invoice within the scope of 230
When anyone has an obligation to protect their vital interests	Giving the health information of the board member who fainted at the board of directors to the doctor
In cases where we need to enter into a contract with you, fulfill the contract, and fulfill our obligations under a contract	Obtaining the customer's bank account information within the scope of the contractual relationship with the customer
Fulfilling our legal obligations,	Fulfillment of our tax obligations, submission of information requested by court decision to the court
If your personal data has been made public by you	To send us e-mails to communicate with you, to write the contact information of the employee candidate to the website where the job application is collected, to use personal data that you have made public through social media channels for the purpose of making them public.
We are obliged to process data for the establishment or protection of a right, to exercise our legal rights and to defend against legal requests brought against us.	Keeping documents that are proof evidence and using them when necessary

-In situations required by our legitimate interests, provided that it does not harm your fundamental rights and freedoms.

-Ensuring the security of our company communication networks and information, conducting our company activities, detecting suspicious transactions and risk

Legal Reason

To conduct research in order to comply with our rules, to benefit from storage, hosting, maintenance and support services in order to provide IT services in terms of technical and security, to benefit from cloud technology to ensure the efficiency of our company activities and to benefit from the possibilities of technology

Examples

Cases where your Personal Data is processed with explicit consent, we would like to emphasize that if you withdraw your express consent, you will be removed from the commercial membership program where such explicit consent processing is required, and that you will not be able to benefit from the advantages you have benefited from as of the relevant date.

WHEN DO WE SHARE YOUR PERSONAL DATA?

Transfer of Personal Data Domestically

Our company, especially in the transfer of personal data, PDPL. 8, we act in accordance with the decision and relevant regulations stipulated in the PDPL and taken by the Board. As a rule, personal data and private data belonging to data owners cannot be transferred by our Company to other natural persons or legal entities without the express consent of the data subject.

In addition, in cases stipulated in articles 5 and 6 of the PDPL, transfer is possible without the consent of the person concerned. Our company, in accordance with the conditions stipulated in the PDPL and other relevant legislation, and taking the security measures specified in the legislation; (If the person who owns the data are available with a contract signed, the contract in question) unless otherwise regulated in the Law and other relevant legislation or are transferred to third parties in Turkey.

Transfer of Personal Data Abroad

Our company, personal data can be transferred to third parties in Turkey and processed in Turkey, or to be maintained processed outside of Turkey, outsourcing included above in accordance with the conditions prescribed in other places in the law as given and the relevant legislation and in abroad, taking the safety precautions are also transferred. We transfer your personal data abroad by taking necessary technical and administrative measures through cloud computing technology in order to carry out our company activities in the most efficient way and to benefit from the possibilities of technology.

PDPL. As a rule, we seek the explicit consent of data owners for the transfer of personal data abroad. However, PDPL. In accordance with 9, PDPL m. 5/2 or m. The existence of one of the conditions regulated in 6/3 and in the foreign country where personal data will be transferred

a) Adequate protection is available,

b) the presence of an adequate protection and permission to commit in writing to the Board and responsible for the data in the relevant foreign country Turkey in the absence of adequate protection transfers abroad without the explicit consent of the data owner.

In this respect, our Company requires that in exceptional cases where express consent is not sought regarding the transfer of personal data mentioned above, in addition to the conditions of processing and

transfer without consent, sufficient protection is required in the country where the data will be transferred in accordance with the PDPL. The Personal Data Protection Board will determine whether sufficient protection is provided. In the case of the absence of adequate protection, and responsible to undertake an adequate protection of data in both written about foreign countries and Personal Data Protection in Turkey must have the permission of the Board.

Please visit our website www.dpworldyarimca.tr for service providers whose headquarters are located abroad in accordance with this paragraph.

Parties Shared Domestic and Abroad

We share your personal data only if necessary for the following purposes. Except for these situations, we take special care not to share your personal data. The parties with whom we share personal data are as follows:

• **DP World corporate headquarters:** Since we operate under DP World group of companies abroad, your data is shared with or made available to DP World corporate headquarters in Dubai. This sharing will only be done with authorized employees in the respective DP World group company. However, we would like to state that the data sharing we do with DP World corporate headquarters in general is carried out in a way that does not include personal data within the scope of financial reporting on company activities such as company profitability and efficiency. In some special cases, instead of sharing anonymous information with DP World corporate headquarters, we may share personal data (such as sharing damage information to open an insurance claim file). DP World Data Sharing Agreement is signed for the transfer of your personal data to DP World group companies and necessary measures are taken.

• **Service providers and business partners**: It defines the parties with which our company establishes business partnerships for purposes such as sales, promotion and marketing of our Company's services, after-sales support, while conducting its commercial activities. Like many businesses, we work with reliable third parties such as information and communication technology providers, consultancy service providers, cargo companies, travel agencies to ensure that functions and services are carried out in the most efficient and up-to-date manner within the scope of some data processing activities, and in this context, data to carry out our activities We share. This sharing is done in a limited way in order to ensure the fulfillment of the establishment and performance purposes of the business partnership. In order to carry out the activities of our company in the most efficient way and to benefit from the technological possibilities at the maximum level, we use cloud information technologies and in this context, we can process your personal data in Turkey and abroad through companies that provide cloud information

services. The marketing services support firm we share with may be established abroad and within this scope, PDPL. 8 and m. 9, data sharing is carried out with abroad in accordance with the provisions regarding data sharing abroad.

• **Government authorities:** When required by law or when we need to protect our rights, we share your personal data with relevant official, judicial and administrative authorities (tax offices, law enforcement agencies, courts and enforcement office).

• **Private law persons:** Private law persons authorized to receive information and documents from our Company in accordance with the provisions of the relevant legislation can share personal data with a limited purpose within their legal authority (Occupational Health and Safety Company).

• **Professional advisors:** We share your personal data with professional advisors such as banks, insurance companies and brokers, auditors, lawyers, financial advisors and other consultants.

• **Other persons associated with corporate transactions:** from time to time for the conduct of corporate transactions such as the sale of a business owned by our company, reorganization, merger, joint venture, or other disposition of our business, assets or shares (including those in connection with any bankruptcy or similar process) we share your personal data.

SOCIAL ADDITIONS

Our web pages use "social plug-ins" from social networks, including the "Share" button of the provider "Facebook" on facebook.com, operated by Facebook Inc., 1601 S. California Ave, Palo Alto, CA 94304, USA. Plugins usually have the Facebook logo. In addition to Facebook, we use "Google+" plugins (provider: Google Inc., Amphitheater Parkway, Mountain View, CA 94043, USA), "YouTube" (provider: YouTube LLC, 01 Cherry Avenue, San Bruno, CA 94066, USA) , “Twitter” (provider: Twitter, Inc., 1355 Market St, Suite 900, San Francisco, CA 94103, USA), “Pinterest” (provider: Pinterest Inc., 808 Brannan Street, San Francisco, CA 94103, USA) , “LinkedIn” (provider of customers outside the US: LinkedIn Ireland Unlimited Company, Wilton Place, Dublin 2, Ireland).

For privacy reasons, we have consciously made the decision not to use plugins directly from social networks on our website. Instead, we use an alternative technical solution that allows you to determine whether and when information is provided to operators and such social networks. When you visit our web pages, no information is automatically sent to social networks such as Facebook, Google+, Twitter or Pinterest. Only when you actively click the relevant button, your Internet browser connects to the servers of the specified social network. This means clicking on the elements in question and then on the symbol of the social network, so that you consent to your Internet browser communicating with the servers of the social network and sending the user data of that network to the operator. We do not have any influence on the type and scope of data collected by social networks. Please refer to the respective privacy policies of these social networks for the purpose and scope of data collection, and the rights and options regarding the security of your privacy regarding the processing and use of data by the relevant social networks.

Facebook's privacy policies can be found here http://www.facebook.com/about/privacy/ and http://www.facebook.com/help/?faq=186325668085084.

More information about data usage for "Google+," "Youtube" or "Twitter" is available at https://policies.google.com/privacy?hl=en&gl=de or http://twitter.com/privacy, for Pinterest at https://policies.google.com/privacy : https//policy.pinterest.com/tr/privacy-policy, for LinkedIn at https://www.linkedin.com/legal/privacy-policy.

Facebook Corporate Products

DP World may use Facebook advertising services and Facebook Pixel retargeting and communication services from time to time. With the Facebook Corporate Products used, DP World aims to advertise to

you on Facebook and or other platforms associated with Facebook and to make these ads more relevant to you. The data collected in this way remains anonymous for DP World and DP World cannot access any personal data regarding individuals.

However, the collected data is stored and processed by Facebook. Facebook may associate your personal data with your Facebook account and use this data for its own advertising activities (in accordance with the Facebook Personal Data Usage Policy accessible at https://www.facebook.com/about/privacy/). Facebook has ultimate control over data collected through Facebook Advertising Services, Facebook Pixel retargeting and communication services. You can change the settings for Facebook cookie usage and Facebook Pixel retargeting in the settings section of your Facebook account.

https://www.facebook.com/ads/preferences/?entry_product=ad_settings_screen.

Please visit the links below to get information about retargeting pixels and technologies provided by Facebook.

https://www.facebook.com/policy.php

https://www.facebook.com/legal/terms/businesstools#

Google Maps

If you use Google Maps to show you maps and create directions to make your travel easier, we would like to point out that Google Maps is operated by Google Inc., 1600 Amphitheater Parkway, Mountain View, CA 94043, USA.

When you use this service, you consent to Google's collection, processing and use of the information entered by you. The terms regarding the use of Google Maps can be found at http://www.google.com/intl/de_de/help/terms_maps.html.

Web analysis with Google Analytics

This website is owned by Google Inc. ("Google") uses Google Analytics, a web analysis service. Google Analytics uses "cookies", text files that are stored on your computer that analyze your use of the website. The information generated by the cookie about your use of this website (including the shortened IP address) is transmitted to a Google server in the United States and stored there. Google will use this

information to analyze your use of the website, to compile reports on website activity for website operators, and to provide more services related to website and Internet usage. Google will also pass it on to third parties where appropriate, when this information is legally required or when these parties process this information on behalf of Google. Google will not associate your IP address with your IP address in any way.

You can prevent your information from being used by Google Analytics by installing a plug-in on your browser. You can click on the link below which will take you to the Google page: http://tools.google.com/dlpage/gaoptout?hl=de.

Business-Non Contain Personal Data

Login

Registration information is created and processed for statistical purposes every time you log into the web page, which ensures that the user remains anonymous:

• The reference (the web page you accessed this page using the link)

Search expressions (if it is a reference search engine)

IP analysis is performed to determine the country and provider of access

Browser, operating system, installed plug-ins and screen resolution

• Duration of stay on pages

• The specified data are processed by us for legal purposes based on PDPL

• Providing a seamless connection with the web page,

• Ensuring comfortable use of the web page,

• Evaluation of system security and stability and other administrative purposes.

We reserve the right to retrospectively check this information if we become aware of certain signs of illegal use. If no longer required for this purpose, the data will be deleted immediately, and in any case after six months at the latest.

HOW LONG DO WE KEEP YOUR PERSONAL DATA?

We only keep your personal data for as long as necessary to fulfill the purpose for which it was collected. We determine these periods separately for each business process and if there is no other reason to keep your personal data at the end of the relevant periods, we destroy your personal data in accordance with PDPL.

While determining the destruction periods of your personal data, we take into account the following criteria:

• The period accepted as a general practice in the sector in which the data controller operates within the scope of the processing of the relevant data category,

• The period that requires the processing of personal data in the relevant data category and the legal relationship established with the relevant person will continue,

• The period during which the legitimate interest to be obtained by the data controller will be valid in accordance with the law and good faith, depending on the purpose of processing the relevant data category,

• The period during which the risks, costs and responsibilities to be created by storing the relevant data category depending on the purpose of processing,

• Whether the maximum period to be determined is suitable for keeping the relevant data category accurate and up-to-date when necessary,

• The period during which the data controller is obliged to keep personal data in the relevant data category in accordance with his legal obligation,

• The statute of limitations determined by the data controller for asserting a right based on personal data in the relevant data category.

HOW DO WE DISPOSE OF YOUR PERSONAL DATA?

Although personal data has been processed in accordance with the provisions of the relevant law in accordance with Article 138 of the Turkish Penal Code and Article 7 of the PDPL, in case the reasons for processing disappear, it will be deleted based on our Company's own decision or if the personal data owner has a request in this direction, destroyed or anonymize.

In this context, Personal Data Storage and Disposal Policy has been prepared. In cases where our company has the right and / or obligation to preserve personal data in accordance with the provisions of the relevant legislation, it reserves the right not to fulfill the request of the data owner. When personal data are processed by non-automatic means, provided that they are part of any data recording system, the system of physical destruction of personal data so that it cannot be used later is applied while the data is deleted / destroyed. When our company agrees with a person or organization to process personal data on its behalf, the personal data is securely deleted by these persons or organizations in a way that cannot be recovered. Our company can anonymize personal data when the reasons requiring the processing of personal data processed in accordance with the law disappear.

DISPOSAL METHODS OF PERSONAL DATA

Although our company has been processed in accordance with the provisions of the relevant law, in the event that the reasons for its processing disappear, it deletes personal data based on its own decision or upon the request of the personal data owner. Deletion of personal data is the process of making personal data inaccessible and unavailable in any way for the relevant users. All necessary technical and administrative measures are taken by our company to ensure that the deleted personal data are inaccessible and unavailable for the relevant users.

Personal Data Disposal Process

The process to be followed in the process of deleting personal data is as follows:

o Determination of personal data that will constitute the subject of deletion.

o Identifying the relevant users for each personal data using an access authorization and control matrix or a similar system.

o Determining the authorizations and methods of the relevant users such as access, retrieval and reuse.

o Closing and eliminating the access, retrieval and reuse authorization and methods of the relevant users within the scope of personal data.

Data is Kept On	**Explanation**
Personal Data Located On Servers	For those who have expired from the personal data on the servers, the system administrator removes the access authority of the relevant users and deletes them.

Personal Data Located on e-Environment	Those who have expired from the personal data in electronic environment are made inaccessible and unavailable in any way for other employees (relevant users) except the database manager.
Personal Data Located on Physical Environment	Except for the department manager responsible for the document archive, for those who require the storage of personal data kept in a physical environment, it is made inaccessible and unavailable in any way. In addition, the process of darkening is also applied by scratching painting wiping it in an illegible way.
Personal Data Located on Portable devices	Personal data kept in Flash-based storage media, which require their storage, are encrypted by the system administrator and access authorization is given only to the system administrator with encryption keys.Stored in safe environments.

Since personal data can be stored in various recording media, they must be deleted by appropriate methods. Examples are given below:

Application Type Cloud Solutions as a Service (such as Office 365 Salesforce, Dropbox: Data must be deleted by giving a delete command in the cloud system. While performing the said operation, it should be noted that the relevant user is not authorized to retrieve deleted data on the cloud system.

Personal Data on Paper Media: Personal data on paper media should be deleted using the blackout method. The blackout process is done by cutting the personal data on the relevant documents whenever possible, and making them invisible to the relevant users by using fixed ink, which is irreversible and cannot be read with technological solutions.

Office Files on the Central Server: The file must be deleted with the delete command in the operating system or the access rights of the relevant user must be removed on the directory where the file or file is located. It should be noted that the relevant user is not the system administrator at the same time while performing the said operation.

Personal Data on Removable Media: Personal data on flash-based storage media should be stored encrypted and deleted using software suitable for these media.

Databases: Relevant lines containing personal data should be deleted with database commands (DELETE etc.). It should be noted that the relevant user is not also a database administrator while performing the said transaction.

Destruction of Personal Data

Although our company has been processed in accordance with the provisions of the relevant law, in the event that the reasons for its processing disappear, it destroys the personal data based on its own decision or upon the request of the personal data owner. The destruction of personal data is the process of making personal data inaccessible, retrieved and reusable in any way. The data controller is obliged to take all necessary technical and administrative measures regarding the destruction of personal data.

Data Recording Media	**Explanation**
Personal Data in the Physical Environment	Those of the personal data in the paper media that require their storage expire are irreversibly destroyed in the paper trimming machines.

Personal Data on Optical OR Magnetic Media	Personal data on optical and magnetic media data that has expired It is physically destroyed, such as melting, burning or pulverizing. In addition, magnetic media is passed through a special device and exposed to a high magnetic field, making the data on it unreadable.

Physical Destroying:

Personal data can also be processed in non-automatic ways, provided that it is a part of any data recording system. While such data is deleted or destroyed, a system of physical destruction of personal data in a way that cannot be used later is applied.

Secure Deletion from Software: While the data that is processed in fully or partially automatic ways and stored in digital media is deleted / destroyed; Methods are used to delete data from the relevant software in a way that cannot be recovered again.

Secure Deletion by Professional: In some cases, he may agree with an expert to delete personal data on his behalf. In this case, the personal data are securely deleted / destroyed by the person skilled in this field so that they cannot be recovered.

OBSCURATION: Making personal data physically unreadable.

Methods of Destroying Personal Data

In order to destroy personal data, it is necessary to detect all copies of the data and to destroy them one by one using one or more of the following methods, depending on the type of systems in which the data is located:

Local Systems: One or more of the following methods can be used to destroy data on these systems. i) De-magnetizing: It is the process of unreadable distortion of the data on the magnetic media by passing it through a special device and exposing it to a very high magnetic field. ii) Physical Destruction: It is the physical destruction process of optical media and magnetic media such as melting, burning or pulverizing. Data is made inaccessible by processes such as melting, burning, pulverizing or passing the optical or magnetic media through a metal grinder. For solid state discs, if overwriting or de-magnetizing is not successful, this media must also be physically destroyed. iii) Overwriting: It is the process of preventing the recovery of old data by writing random data consisting of 0 and 1 at least seven times on magnetic media and rewritable optical media. This process is done using special software.

Environmental Systems: The destruction methods that can be used depending on the type of media are as follows: İ) Network devices (switches, routers, etc.): The storage media inside these devices are fixed. Products often have a delete command but no destruction feature. It must be destroyed by using one or more of the appropriate methods specified in (a). ii) Flash-based media: Flash-based hard disks that have ATA (SATA, PATA, etc.), SCSI (SCSI Express, etc.)) must be destroyed using one or more of the appropriate methods specified in. iii) Magnetic tape: Media that store data with the help of micro magnet pieces on the flexible tape. It must be destroyed by exposure to very strong magnetic media and de-magnetizing or physical destruction methods such as burning or melting. iv) Units such as magnetic discs: Media that store data with the help of micro-magnet parts on flexible (plate) or fixed media. It must be destroyed by exposure to very strong magnetic media and de-magnetizing or physical destruction methods such as burning or melting. v) Mobile phones (Sim card and fixed memory areas):

Portable smartphones have a delete command in fixed memory areas, but most of them do not have a destroy command. It must be destroyed by using one or more of the appropriate methods specified in (a). vi) Optical discs: These are data storage media such as CDs and DVDs. It must be destroyed by physical destruction methods such as burning, breaking into small pieces, melting. vii) Peripherals such as printers with removable data recording media, fingerprint door access system: All data recording media must be verified to be removed and destroyed by using one or more of the appropriate methods specified in (a) according to their characteristics. viii) Peripherals such as printer, fingerprint door access system with fixed data recording medium: Most of these systems have a delete command, but there is no destroying command. It must be destroyed by using one or more of the appropriate methods specified in (a).

Paper and Microfiche Media: The main media must be destroyed since the personal data in these media is permanently and physically written on the media. While performing this process, it is necessary to divide the media into small pieces that are incomprehensible with paper shredding or shearing machines, horizontally and vertically if possible, so that they cannot be put back together. Personal data transferred from the original paper format to the electronic environment by scanning should be destroyed by using one or more of the appropriate methods specified in (a), depending on the electronic environment in which they are located.

Cloud Environment: During the storage and use of personal data in these systems, encryption with cryptographic methods and where possible for personal data, especially for each cloud solution service

Making Personal Data Anonymous

Anonymization of personal data means making personal data unrelated to a certain or identifiable natural person under any circumstances, even by matching with other data. Our company can anonymize personal data when the reasons requiring the processing of personal data processed in accordance with the law disappear. In order for personal data to be anonymize; Personal data must be rendered unrelated to an identified or identifiable natural person, even through the use of appropriate techniques in terms of the recording medium and the relevant field of activity, such as the return of personal data by the data controller or recipient groups and / or matching the data with other data. Our company takes all kinds of technical and administrative measures required to anonymize personal data.

PDPL. In accordance with 28; Anonymize personal data can be processed for purposes such as research, planning and statistics. Such processes are outside the scope of PDPL and the explicit consent of the personal data owner will not be sought.

Anonymizing Methods of Personal Data

The anonymization of personal data is the rendering of personal data that cannot be associated with an identified or identifiable natural person under any circumstances, even if they are matched with other data.

In order for personal data to be anonymized; Personal data must be rendered unrelated to an identified or identifiable natural person, even through the use of appropriate techniques in terms of the recording medium and the relevant field of activity, such as the return of personal data by the data controller or third parties and / or matching the data with other data.

Business-Non Contain Personal Data

Anonymization is the removal or modification of all direct and / or indirect identifiers in a data set, preventing the identification of the relevant person from being identified or losing its distinctiveness within a group or crowd in a way that cannot be associated with a real person. Data that do not point to a specific person as a result of blocking or losing these features are considered anonymized data. In other words, while the anonymized data was the information identifying a real person before this process was carried out, it became unrelated to the relevant person after this process and was disconnected from the person. The purpose of anonymization is to break the link between the data and the person identified by this data. Anonymization methods are all of the link breakage processes carried out by methods such as automatic or non-automatic grouping, masking, derivation, generalization, randomization applied to the

records in the data recording system where personal data are kept. The data obtained as a result of the application of these methods should not be able to identify a specific person.

Examples of anonymization methods are described below:

Anonymization Methods That Do Not Provide Value Irregularities: In methods that do not provide value irregularities, a change or addition or subtraction is not applied to the values of the data in the set, instead, changes are made to the entire row or column in the set. Thus, while the overall data changes, the values in the fields maintain their original state.

Removing Variables

It is a method of anonymization provided by removing one or more of the variables from the table completely. In such a case, the entire column in the table will be removed completely. This method can be used for reasons such as the variable being a high-grade descriptor, the lack of a more appropriate solution, the variable being too sensitive data to be disclosed to the public, or not serving analytical purposes.

Removing Records

In this method, anonymity is strengthened by removing a line containing singularity in the data set and the possibility of generating assumptions about the data set is reduced. Generally, the extracted records are records that do not share a common value with other records and that people who have an idea about the data set can easily guess. For example, in a dataset containing survey results, only one person from any industry is included in the survey. In such a case, instead of removing the "sector" variable from all survey results, it may be preferable to remove only the record belonging to this person.

Regional Concealment

The purpose of the regional hiding method is to make the data set more secure and reduce the risk of predictability. If the combination of values belonging to a particular record creates a poorly visible situation and this may cause that person to become highly distinguishable in the relevant community, the value that creates the exception is changed to “unknown”.

Generalization

It is the process of converting the relevant personal data from a special value to a more general value. It is the most used method when generating cumulative reports and in operations carried out over total

numbers. The new values obtained as a result show the total values or statistics of a group that makes it impossible to reach a real person. For example, if a person with TR ID Number 12345678901 bought diapers from the e-commerce platform, he also bought wet wipes. In the anonymization process, by using the generalization method, it can be concluded that % of the people who buy diapers from the e-commerce platform also Lower and Upper Limit Coding

The lower and upper limit coding method is obtained by defining a category for a certain variable and combining the remaining values in the grouping created by this category. Usually, the low or high values of a certain variable are added together and a new definition is made to these values.

Global Coding

The global coding method is a grouping method used in data sets that do not contain numerical values or cannot be numerically ordered, where lower and upper bound coding is not possible. It is generally used when certain values are clustered to make it easier to make estimates and assumptions. By creating a common and new group for the selected values, all records in the data set are replaced with this new definition.

Sampling

In the sampling method, instead of the whole data set, a subset from the set is explained or shared. Thus, since it is not known whether a person known to be included in the entire data set is included in the disclosed or shared sample subset, the risk of producing accurate predictions about individuals is reduced. Simple statistical methods are used to determine the subset to be sampled. For example; It may be meaningful to make scans and make predictions in the relevant data set about a woman who is known to live in Istanbul, if a data set on demographic information, professions and health conditions of women living in Istanbul is anonymized or shared. However, in the relevant data set, only the records of women whose registration is in Istanbul are left, and if the birth registration is removed from the data set and the data is disclosed or shared, the malicious person who accesses the data is in Istanbul. Since the information belonging to this person he knows is not included in the data in his possession or not, he will not be able to make a reliable estimate of whether the information is included buy wet wipes.

Anonymization Methods Providing Value Irregularity: Different from the methods that provide value disorder; Distortion is created in the values of the data set by changing the existing values. In this case, since the values of the records are changing, the benefit planned to be obtained from the data set must be calculated correctly. Even if the values in the data set are changing, it can still be benefited from the data by ensuring that the total statistics are not corrupted.

Micro Joining

With this method, all records in the data set are first arranged in a meaningful order and then the whole set is divided into a certain number of subsets. Then, the average value of each subset of the specified variable is taken and the value of that variable of the subset is replaced with the average value. Thus, the average value of that variable for the entire data set will not change.

Data Exchange

The data exchange method is the record changes obtained by exchanging the values of a variable subset between the pairs selected from the records. This method is mainly used for variables that can be

categorized and the main idea is to transform the database by changing the values of the variables between the records of individuals.

Adding Noise

With this method, additions and subtractions are made to provide a determined degree of distortion in a selected variable. This method is mostly applied to data sets containing numerical values. Distortion applies equally to each value.

Statistical Methods To Strengthen Anonymization

As a result of the combination of some values in the records with single scenarios in the anonymized data sets, the possibility of identifying the persons in the records or deriving assumptions about their personal data may arise.

For this reason, anonymity can be strengthened by minimizing the singularity of the records in the data set by using various statistical methods in the anonymized data sets. The main purpose of these methods is to minimize the risk of deterioration of anonymity while keeping the benefit from the data set at a certain level.

K-Anonymity

In the anonymized data sets, when indirect identifiers are combined with the right combinations, the identities of the persons in the records can be determined or the information about a particular person can be easily predicted has shaken the trust in the anonymization processes. Accordingly, the data sets that were anonymized by various statistical methods had to be made more reliable. K-anonymity has been developed to prevent disclosure of information specific to individuals that show singular characteristics in certain combinations by enabling the identification of more than one person with certain fields in a data set. If there is more than one record of combinations created by combining some of the variables in a data set, the probability of identifying the persons corresponding to this combination decreases.

L-Diversity

The L-diversity method, which is formed by studies conducted on the shortcomings of K-anonymity, takes into account the diversity created by sensitive variables corresponding to the same variable combinations.

T-Proximity

Although the L-diversity method provides diversity in personal data, there are situations where it cannot provide sufficient protection because the method does not deal with the content and sensitivity of personal data. In this way, the process of calculating the degree of closeness of personal data within the values and making the data set anonymized by dividing it into subclasses according to these degrees of closeness is called the T-proximity method.

Choosing the Anonymization Method

Our company decides which of the above methods will be applied by looking at the data in their possession and considering the following features regarding the owned data set;

The nature of the data,

The size of the data,

The nature of the data in physical environments,

Data diversity,

The desired benefit , processing purpose from the data,

Data processing frequency,

The reliability of the party to whom the data will be transfer,

The effort to be made to anonymize the data is meaningful,

The magnitude of the damage that may occur if the anonymity of the data is broken, its area of influence,

The distribution ,centralization rate of the data,

User's access authorization control and

The possibility that the effort he will spend to construct and implement an attack that will disrupt anonymity will be meaningful.

When a data is anonymized, our Company checks whether the data is known to be within the structure of other institutions and organizations to which it transmits personal data or whether it is publicly available, through contracts and risk analysis.

Anonymity Assurance

While our company decides to anonymize a personal data instead of deleting or destroying it, the anonymity cannot be disrupted by combining the anonymized data set with a thousand other data sets, not creating a meaningful whole that can make a record of one thousand or more values singular, anonymized. The values in the data set do not merge to produce an assumption or result, and the data sets anonymized by our company are checked as the features listed in this article change, and it is ensured that anonymity is preserved.

Risks of Disrupting Anonymization by Reverse Processing of Anonymized Data

Since the anonymization process is applied to personal data and destroys the distinctive and identifying features of the data set, there is a risk that these transactions will be reversed by various interventions and the anonymized data will become identifiable and distinctive to real persons. This situation is expressed as anonymity breakdown. Anonymization can only be achieved by manual processes or automatically enhanced processes, or by hybrid processes that are a combination of both types of transactions. However, what is important is that after the anonymized data is shared or disclosed, measures have been taken to prevent the anonymity from being corrupted by new users who can access or own the data. The actions carried out consciously regarding the deterioration of anonymity are called “attacks against anonymity”. In this context, it is investigated whether there is a risk of reversing personal data that has been anonymized by our Company with various interventions and that the

anonymized data will become re-identifying and distinguishing real persons, and the process is established accordingly.

HOW DO WE PROTECT YOUR PERSONAL DATA?

Necessary administrative and technical measures are taken by our Company in line with the Personal Data Security Guide published by the PDP Institution in order to protect and prevent unlawful access of your personal data, procedures are arranged within the Company, clarification and explicit consent texts are prepared and PDPL article. In accordance with 12/3, necessary inspections are carried out or outsourced to ensure the implementation of the provisions of the PDPL. These audit results are evaluated within the scope of the internal functioning of the Company and necessary actions are taken to improve the measures taken.

Your personal data mentioned above can be transferred to the physical archives and information systems of our Company and / or our suppliers and kept in both digital and physical environment. The technical and administrative measures taken to ensure the security of personal data are explained in detail below under two headings.

Technical Measures

We use generally accepted standard technologies and business security methods, including standard technology called Secure Socket Layer (SSL), for the protection of personal information collected. However, due to the nature of the Internet, information can be accessed by unauthorized persons over the networks without the necessary security measures. Depending on the current state of technology, the cost of technological implementation and the nature of the data to be protected, we take technical and administrative measures to protect your data from risks such as destruction, loss, tampering, unauthorized disclosure or unauthorized access. In this context, we conclude agreements with the service providers we work with regarding data security. You can find detailed information about these service providers via.

1. Ensuring Cyber Security: We use cyber security products to ensure personal data security, but the technical measures we take are not limited to this. With measures such as firewall and gateway, the first line of defense against attacks from environments such as the Internet is established. However, almost all software and hardware are subjected to some installation and configuration processes. Considering that some commonly used software, especially old versions, may have documented security vulnerabilities, unused software and services are removed from the devices. For this reason, deletion of unused software and services is preferred primarily because of its ease, rather than keeping it up-to-date. With patch management and software updates, it is ensured that the software and hardware work properly and that the security measures taken for the systems are checked regularly.

2. **Access Limitations**: Access authorizations to systems containing personal data are restricted and regularly reviewed. In this context, employees are given access to the extent necessary for their job and duties, as well as their powers and responsibilities, and access to relevant systems is provided by using a username and password. While creating the said passwords and passwords, it is ensured that combinations consisting of uppercase letters, numbers and symbols are preferred instead of numbers or letter strings that are associated with personal information and are easy to guess. Accordingly, access authorization and control matrix is created.

3.**Encryption**: In addition to the use of strong passwords and passwords, limiting the number of password entry attempts to protect against common attacks such as the use of brute force algorithm (BFA), ensuring that passwords and passwords are changed at regular intervals, opening the administrator account and admin authority only when needed. and for employees who are dismissed from the data controller, access is limited by methods such as deleting the account or closing the entries without losing time.

4.**Anti Virus Software**: In order to protect against malicious software, products such as antivirus and antispam are used that regularly scan the information system network and detect threats, and they are kept up-to-date and necessary files are regularly scanned. If personal data is to be obtained from different websites and / or mobile application channels, it is ensured that the connections are made via SSL or a more secure way.

5. **Monitoring of Personal Data Security:** Checking which software and services are running in information networks, Determining whether there is an infiltration or non-infiltration in information networks, Recording transactions of all users (such as log records), Security problems as quickly as possible reporting, done. Again, a formal reporting procedure is established for employees to report security weaknesses in systems and services or threats that use them. Evidence is collected and securely stored in unwanted events such as the collapse of the information system, malicious software, denial of service attack, incomplete or incorrect data entry, violations that disrupt privacy and integrity, and abuse of the information system.

6. Ensuring the Security of Media Containing Personal Data: If personal data is stored on devices located in the campuses of data controllers or in paper environment, physical security measures are taken against threats such as theft or loss of these devices and papers. Physical environments containing personal data are protected against external risks (fire, flood,etc.) with appropriate methods and entry , exit to these environments is controlled.

If personal data is in electronic environment, access can be restricted between network components or the components are separated in order to prevent personal data security breach. For example, if personal data is processed in this area by restricting it to a certain part of the network that is used only for this purpose, available resources may be reserved for the purpose of securing this limited area, not for the entire network.

Measures at the same level are also taken for paper media, electronic media and devices located outside the Company campus and containing personal data belonging to the Company. As a matter of fact, although personal data security violations often occur due to the theft and loss of devices (laptop, mobile phone, flash disk, etc.) containing personal data, personal data to be transferred by e-mail or mail are also sent carefully and with sufficient precautions. In case employees access the information system network with their personal electronic devices, adequate security measures are taken for them as well.

The method of using access control authorization and / or encryption methods is applied against cases such as the loss or theft of devices containing personal data. In this context, the password key is stored in an environment that only authorized persons can access and unauthorized access is prevented.

Paper documents containing personal data are also stored in a locked way and in environments that can only be accessed by authorized persons, and unauthorized access to such documents is prevented.

Our company, PDPL m. 12, if the personal data is obtained by others through illegal means, it notifies the PDP Board and data owners as soon as possible. The PDP Board, if it deems necessary, may announce this on the website or by any other method.

7. Storage of Personal Data in the Cloud: In case personal data is stored in the cloud, the Company should evaluate whether the security measures taken by the cloud storage service provider are sufficient and appropriate. In this context, two-stage authentication control is applied for knowing in detail what personal data stored in the cloud is, backing up, ensuring synchronization and remote access to these personal data if required. During the storage and use of personal data in these systems, it is ensured that personal data are encrypted with cryptographic methods, encrypted and disposed of in cloud environments, and where possible for personal data, in particular, separate encryption keys are used for each cloud solution service is provided. When the cloud computing service relationship ends; All copies of encryption keys that could be used to make personal data usable are destroyed. Access to data storage areas where personal data is stored are logged and inappropriate access or access attempts are instantly communicated to those concerned.

8. Procurement, Development and Maintenance of Information Technology Systems: Security requirements are taken into consideration while determining the needs of the company regarding the procurement, development or improvement of existing systems.

9) Backing Up Personal Data: In cases where personal data is damaged, destroyed, stolen or lost for any reason, the Company ensures that the data is backed up as soon as possible. Backed up personal data can only be accessed by the system administrator, and data set backups are excluded from the network.

Administrative Measures

• All activities carried out by our company were analyzed in detail for all business units and as a result of this analysis, a process-based personal data processing inventory was prepared. Risky areas in this inventory are identified and necessary legal and technical measures are taken continuously. (For example, documents required to be prepared within the scope of PDPL have been prepared by considering the risks in this inventory)

• Personal data processing activities carried out by our company are audited by information security systems, technical systems and legal methods. Policies and procedures regarding personal data security are determined and regular controls are carried out within this scope.

• Our company may receive services from external service providers from time to time in order to meet its information technology needs. In this case, the transaction is made by making sure that the said Data Processing external service providers at least meet the security measures provided by our Company. In this case, this contract, signed by signing a written contract with the Data Processor, includes at least the following points:

o The Data Processor acts only in accordance with the Data Controller's instructions in accordance with the purpose and scope of data processing specified in the contract and in accordance with the PDPL and other legislation,

o Acting in accordance with the Personal Data Storage and Destruction Policy,

o The Data Processor is subject to an indefinite confidentiality obligation regarding the personal data processed,

o In case of any data breach, the Data Processor is obliged to immediately notify the Data Supervisor of this situation,

o Our Company will make or have the necessary audits on the systems of the Data Processor containing personal data, and can examine the reports and the service provider company on site,

o It will take necessary technical and administrative measures for the security of personal data; and

o In addition, as the nature of the relationship between the Data Processor and us permits, the categories and types of personal data transferred to the Data Processor are also specified in a separate article.

• As the Institution emphasizes in its guides and publications, within the framework of the principle of data minimization, personal data are reduced as much as possible and unnecessary, outdated and not serving a purpose is not collected, and if it was collected in the period before the PDPL, a compliant with the Personal Data Storage and Destruction Policy it is destroyed.

• Personnel who are experts in technical matters are employed.

• Our company has determined provisions regarding confidentiality and data security in the Employment Agreements to be signed during the recruitment process of our employees and asks employees to comply with these provisions. Employees are regularly informed and trained on the law on protection of personal data and taking necessary measures in accordance with this law. The roles and responsibilities of the employees were reviewed within this scope and their job descriptions were revised.

• Technical measures are taken in line with technological developments, the measures taken are periodically checked, updated and renewed.

• Access authorizations are limited and the authorities are regularly reviewed.

• The technical measures taken are regularly reported to the officer, and efforts are made to produce the necessary technological solutions by reviewing the issues that pose risks.

• Software and hardware including virus protection systems and firewalls are installed.

• Backup programs are used to ensure the safe storage of personal data.

• Security systems for storage areas are used, technical measures taken are periodically reported to the relevant person as required by internal controls, issues that pose a risk are re-evaluated and necessary technological solutions are produced. The files, outputs stored in the physical environment are kept by the supplier companies and then destroyed in accordance with the determined procedures.

• The issue of Personal Data Protection is also owned by the senior management, a special Committee has been established (PDP Committee) and started to work. A management policy regulating the

working rules of the Company's PDP Committee has been put into effect within the Company and the duties of the PDP Committee have been explained in detail.

HOW DO WE PROTECT YOUR SPECIAL QUALITY PERSONAL DATA?

Separate policy regarding the processing and protection of special quality personal data has been prepared and put into effect.

PDPL m. 6, data on race, ethnicity, political opinion, philosophical belief, religion, sect or other beliefs, attire, association, foundation or union membership, health, sexual life, criminal conviction and security measures, and biometric and genetic data are subject to law. Since they have the risk of causing victimization or discrimination when processed inappropriately, it has been organized as special quality personal data and the processing of this data is subject to a more sensitive protection.

Our company enlightens the Relevant Persons during the acquisition of special quality personal data in accordance with Article 10 of the PDPL. Special quality personal data are processed by taking measures in accordance with the PDPL and by carrying out the necessary inspections. As a rule, one of the conditions for processing special personal data is the explicit consent of the data owner. Our company offers data owners the opportunity to express their explicit consent on a specific subject, based on information and with free will.

As a rule, our company obtains the express consent of the Related Persons in writing for the processing of special quality data. However, PDPL m. In accordance with 6/3, PDPL m. In the presence of any of the conditions specified in 5/2, the explicit consent of the Related Persons is not required. Besides, PDPL m. 6/3, for the protection of public health, preventive medicine, medical diagnosis, treatment and care services, planning and management of health services and financing of personal data related to health and sexual life, by persons under the obligation of secrecy or authorized institutions and organizations, regulates that it can be processed without seeking consent. Regardless of the reason, general data processing principles are always taken into account in processing processes and compliance with these principles is ensured.

Our company takes special measures to ensure the security of sensitive personal data. In accordance with the principle of data minimization, special quality personal data are not collected unless necessary for the relevant business process and are processed only when necessary. In case of processing special quality personal data, necessary technical and administrative measures are taken to comply with legal obligations and to comply with the measures determined by the PDP Board.

WHAT ARE YOUR RIGHTS REGARDING YOUR PERSONAL DATA?

PDPL as data owners, you have the following rights regarding your personal data:

• Learning whether your personal data is being processed by our Company,

• If your personal data has been processed, to request information regarding this,

• Learning the purpose of processing your personal data and whether they are used appropriately for their purpose,

Knowing the third parties in the country or abroad to whom your personal data has been transferred,

• To request correction of your personal data in case of incomplete or incorrect processing, and to request notification of the transaction made within this scope to third parties to whom your personal data has been transferred,

• To request the deletion or destruction of your personal data in the event that the reasons requiring its processing disappear, despite the fact that it has been processed in accordance with the provisions of PDPL and other relevant laws, and to request the third parties to whom your personal data has been transferred,

• Object to the occurrence of a result against you by analyzing the processed data exclusively through automated systems,

• To request the compensation of the damage you suffered in case you suffer damage due to the illegal processing of your personal data.

You can send these requests to our Company free of charge in accordance with the Application Communiqué by the method stated below:

1) Visit www. ...com address filled in the present form in DP World, after being signed as a wet signature Yarımca Port Operations Inc. Mimar Sinan neighborhood Mehmet Akif Ersoy street No: 168, 41780 Yarımca Gulf - Turkey address the person transmitting (We would like to remind you that your ID will need to be presented.

2) www. .. .com After filling the form available at the address signed are signed by DP World Yarımca Port Operations Inc. Mimar Sinan neighborhood Mehmet Akif Ersoy street No: 168, 41780 Yarımca Gulf - Turkey address to the notary means sending.

3) Filling in the application form at www. .. .com.tr and signing with your "secure electronic signature" within the scope of Electronic Signature Law No. 5070, sending the secure electronic signed form to dpworld@hs01.kep.tr via registered e-mail.

4) Submission in writing using your e-mail address previously notified to our company and registered in

In the application;

Name, Last Name , and the application is written signature, to the citizens of the Republic of Turkey T. R. Identity Number, nationality for foreigners, passport number or identification number, if any, place of residence or workplace address for notification, e-mail address for notification, telephone and fax number, subject of request, if any, must be present. Information and documents on the subject are also attached to the application.

It is not possible to make requests by third parties on behalf of personal data owners. In order for a person other than the personal data owner to make a request, a wet signed and notarized copy of the special power of attorney issued by the personal data owner in the name of the person who will make the application must be available. In the application containing your explanations regarding the right you have as a personal data owner and that you will make to exercise your rights stated above and that

you request to use; The subject you request must be clear and understandable, the subject you request is related to your person, or if you are acting on behalf of someone else, you must be specially authorized and document your authorization, the application must include your identity and address information and documents that prove your identity must be attached to the application.

Your applications within this scope will be finalized in the shortest possible time frame and within 30 days at the most. These applications are free of charge. However, if the transaction requires an additional cost, the fee in the tariff determined by the PDP Board may be charged.

If the personal data owner submits his request to our Company in accordance with the prescribed procedure, our Company will conclude the relevant request free of charge as soon as possible and within thirty days at the latest, depending on the nature of the request. However, if the transaction requires an additional cost, the fee in the tariff determined by the PDP Board will be collected from the applicant by our Company. Our company may request information from the person concerned in order to determine whether the applicant is the owner of personal data. In order to clarify the matters in the application of the personal data owner, our company may ask a question to the personal data owner about his application.

PDPL m. 14, if your application is rejected by our Company, you find our answer inadequate or we do not reply to the application in time; You can complain to the PDP Board within thirty days from the date you learn the response of our company, and in any case, within sixty days from the date of application.

WHAT ARE THE SITUATIONS WHERE DATA OWNERS CANNOT EXTEND THEIR RIGHTS?

Personal data owners cannot claim the above-mentioned rights of personal data owners in these matters, since the following situations are excluded from the scope of PDPL in accordance with Article 28 of the PDPL:

o Processing personal data for purposes such as research, planning and statistics by anonymizing them with official statistics.

o Processing of personal data for artistic, historical, literary or scientific purposes or within the scope of freedom of expression, provided that they do not violate national defense, national security, public security, public order, economic security, privacy of private life or personal rights or constitute a crime.

o Processing of personal data within the scope of preventive, protective and intelligence activities carried out by public institutions and organizations authorized by law to ensure national defense, national security, public security, public order or economic security.

o Processing of personal data by judicial authorities or execution authorities in relation to investigation, prosecution, trial or execution proceedings.

In accordance with the article 28/2 of the PDPL; In the cases listed below, personal data owners cannot assert their other rights, except the right to demand compensation:

o Processing of personal data is necessary for the prevention of crime or for a criminal investigation.

o Processing of personal data made public by the personal data owner himself.

o Processing of personal data is necessary for the execution of supervision or regulation duties and disciplinary investigation or prosecution by the authorized and authorized public institutions and organizations and professional organizations having the status of public institutions, based on the authority granted by law

o Processing of personal data is necessary for the protection of the economic and financial interests of the State regarding budget, tax and financial issues.ompany's system.

OTHER ISSUES

As explained in detail above, your personal data can be stored and preserved, classified as required by market research, financial and operational processes and marketing activities, updated in different periods and, to the extent permitted by the legislation, within the framework of laws and confidentiality principles, third parties and / or suppliers and / or services Providers and / or foreign shareholders to whom we are affiliated, information can be transferred, stored and processed by reporting, in accordance with the policies we are affiliated with and for the reasons stipulated by other authorities, records and documents can be prepared in an electronic or paper environment as a basis for processing.

In case of inconsistency between the provisions of PDPL and other relevant legislation and this Policy, the provisions of the PDPL and other relevant legislation will be applied first.

This Policy prepared by our company has entered into force pursuant to the decision taken by the DP World Board of Directors.

Effective Date: 1.1.2019

Version: 1

ABBREVIATIONS	
Law No. 5651	The Law on Regulating Publications on the Internet and Combating Crimes Committed Through These Publications, which entered into force after being published in the Official Gazette No. 26530 dated 23 May 2007
Constution	Dated November 9, 1982 and published in the Official Gazette No. 17863 dated November 7, 1982 and No. 2709 Constitution of Turkey.
Application Notice	On Application Procedures and Principles for the Data Controller, which entered into force after being published in the Official Gazette No. 30356 dated March 10, 2018
Relevant Person / Relevant Persons or Data Owner	Customers of DP World and DP World affiliated group companies are limited to corporate customers, business partners, shareholders, officials, candidate employees, interns, visitors, suppliers, employees of the institutions they cooperate with, third parties and those listed here. It refers to the real person whose personal data is processed like other persons.
Regulation on Deletion, Destruction or Anonymization of Personal Data	Regulation on Deletion, Destruction or Anonymization of Personal Data, published in the Official Gazette dated October 28, 2017 and numbered 30224 and entered into force as of January 1, 2018

Business-Non Contain Personal Data

PDPL	The Law on Protection of Personal Data published in the Official Gazette dated April 7, 2016 and numbered 29677
PDP Board	Personal Data Protection Board
PDP Instution	Personal Data Protection Authority
Art	Article
Ex	Example
Policy	This DP World Personal Data Protection and Privacy Policy
Company / DP World	DP World Yarımca Port Management Incorporated Company
Turkish Penal Law	Published in the Official Gazette No. 25611 dated October 12, 2004; Turkish Penal Law No. 5237 of 26 September 2004

Business-Non Contain Personal Data