Internal GDPR Policy

Document№.	**Melon-GDPR- 1.1**
Version:	**1**
Data:	**24.September 2018**
Issued:	
Owner of the document	

Content

Introduction

The administrator Melon AD (**the Company**) gathers and uses individuals' personal data due to the different relationships of **the Company** with the personal data subjects. Some of the examples can be seen below and a detailed description can be found in Personal Data Inventory

- Employees;
- Clients;
- Different contracted service suppliers;
- Website users managed by **the Company** used for an easy-going business process;
- The collected personal data are being transferred to third party side described in details in Personal Data Inventory;

Aim of the policy

This policy aims to describe the ways and the standards of collecting, processing and preserving personal data so that keeping the certain legislation can be guaranteed

The present policy aims to guarantee the following:

- Creating premises, processes and requirements for applying good practices for following the applicable legislation in the GDPR area. Which by the time of creating the present document, consists of the common GDPR 2016/679 (the Regulation), the low of personal data protection acting since 01.01.2002 (the Law) sub law and normative acts (all called Legislation
- Creates transparency in terms of the ways in which the personal data is being kept and processed;
- Ensures protection of the personal data on projecting stage and by default
- Guarantees the rights personal data holders, users, clients, employees, services suppliers and partners.
- Ensures procedures for duties performing on behalf of **the Company** in case there is a personal data breach and leak.

Principles lying in the Regulation

The Regulation defines a few main principles, with obligatory character:

1. Legality, integrity and transparency (p. 29 from the Preamble).

These principals have their main application in clear, on time, detailed and thorough subjects informing of the ways in which the personal dat5at related to them is being collected, used, consulted or processed in any other way as well as the range in which the personal data processing is being done or will be done.

The Company has created a number of policies and premises granting easy accessible and understandable informing of the subjects about the range, the concrete purposes, risks, rules and processing guarantees,

Furthermore, all the main points because of which such relationships of collecting, keeping and processing of personal data arise have been reviewed and suitable for each of them solutions have been found.

Main challenges in performing this obligation **the Company** finds in the following activities:

- Working with mobile app users , website users and online users of **the Company** that traditionally have been and are objects of collecting and processing personal data In order to ensure they being informed and their personal data being protected **the Company** has designed a special process where each website or online visitor a pop up is being visualized where all the concrete aims of collecting personal data are being described and for all of them excluding the absolutely necessary ones for the normal operation of the website or for fulfilling contract obligation an agreement is being asked for.
- Projects realization containing arrays or fragments with personal data. By exception **the Company** fulfils such projects for the successful developing of which working with personal data is required. The personal data is given by the assignors of such projects with no exception which implies suitable arrangements with them
- The process of transferring information with the office of **the Company** in the Republic of Macedonia. In order to answer the law requirements all processes must be assessed and the transferred in their context personal data and claims for the operation so that the specific law requirements of the Regulation are kept.

The transmit of the personal data after an agreement has been made by the subjects is strictly controlled and all measures for preserving their immunity have been taken. For this purpose, **the Company** has adopted a number of policies such as Policy for information security; Policy for web security; Policy for defense against malfunctioning software; Cryptography Policy; Policy for access control etc.

A different number of policies and procedures5 is being applied to the employees starting with evidential paper informing and an agreement for processing their personal data is also taken for the purposes of performing their labor and civil contracts and apart from that where there is a will on behalf of the subjects for additional aims including secondary processing.

The protection of the secureness of the personal data is being granted once by the already mentioned above policies but also from the procedures and the policies implemented in ISO 270001.

2. Minimizing of the data

When collecting data, **the Company** and its employees must take into consideration the Regulation's requirement the collected data to be in as minimalistic volumes as possible. Along with this the business specifics for websites and mobile apps for users developing and maintenance will be considered.

Since the process for minimalizing data is complicated **the Company** expectations are that it will last longer including after the Regulation come to life. To ensure correct understanding on behalf

of the employees and defining the practical requirements towards this regulated obligation the procedures and the policies implemented in GDPR and ISO 27001 have been developed.

Restricting the goals

Personal data must be collected purely for concrete and lawful purposes and not to be processed later on for purposes other than the ones already mentioned.

Main challenges are:

- Website visitors, online and mobile app visitor's personal data. There is a typical for the online projects' combination between lightening thorough and detailed collecting of personal data and metadata which could support profiling or identifying of the subjects within combinations with other data related to them. This is why setting up a clear stricture for the concrete purposes of collecting is a must along with mechanisms of taking an agreement by the users and keeping the limits set by the collected agreements in terms of collecting, keeping and processing and transferring personal data. Specific issues arise by using standard for the industry tools for measuring the users behavior which collect and use personal and metadata. For resolving those a standardized set of concrete purposes for agreement has been developed for which the website users, the online tools and mobile app users cast their agreement and only after it has been collected usage of specific 3rd party tools begin;
- Personal data disposed by project assignors **The Company**;
- Tests individually each project and assures that its completion would have been either impossible or significantly difficult without using real bases or fragments containing personal data. If this is undoubtably established next step towards overviewing the practices, the methodology and the reasons for collecting the subject's agreement is being taken on behalf of the assignor and the particular written guarantees are being collected. That the agreement casting has been done in line with the Regulation and the applying legislation Suitable and preferred for **the Company** form is the modal one when defining clauses in the contracts.
- Process of transferring information with the office in Republic of Macedonia. The personal data transfer is available on certain of directions
    - Employee data. The range of the personal data which is to be transferred is defined by the special committee on every 6 months. According the specific requirements. All the high Management of **the Company** takes part in this committee as well as the HR teams, the Finance team, Trade and Law teams. As a result of its activity a number of situations is being generated require wing transfer of personal data, the different personal data categories are being described in details along with the motives for the transfer. Forms for the employees are being created which have the purpose to notify them about the transfer and its details and to give their agreement before the transfer takes place.
    - Personal data given by assignors in terms of solution development Before such transfer takes place **the Company** conducts risk assessment and analyzes the need of transfer of personal data 9or fragments or metadata the transfer range and the given evidence and guarantees by the assignor that all the necessary

agreements for the transfer outside the EEZ have been taken The risk assessment analysis is prepared by employee initiative by GDPR and of course relevant specialists also take part in this. The report is then approved by the High Management

- Personal data, fragments and metadata with the potential to identify the mobile app users, website users and the online products of **the Company** users. The personal data transfer collected by these channels could be applied by the needs of internal processes (product and service analysis, marketing etc.). For this purpose **the Company** has added suitable texts in its requirements towards its employees and those in the office in Republic of Macedonia formalized under the form of texts in labor contracts, job description, declarations when starting a job and declarations related to project participation.

3. Accuracy of the data

The accuracy of data as a requirement of the **Regulation** is not a significant issue for **the Company** excluding the activities related to websites and online products of **the Company**.

Opportunities to correct their personal data in their access profiles to websites and online products have been created as well as the possibility to ask for correction of the presenting website of **the Company** by specifically implying for which of data they would like a correction

Option has been given to the partners and the assignors from whom personal data, fragments or metadata is received to delegate towards **the Company** requests for personal data correction received by them.

Employees can ask for a correction of their personal data from Human resources department through specific form.

4. Maximum time range for keeping the data determination.

The Regulation requires clear definition of the terms for keeping personal data. The different personal data categories and specific purposes of their processing require a specific procedure based on the data in *Personal data inventory and Mapping the personal data streams* as well as the created in *Policy of terms for keeping personal data*, *anonymizing personal data procedure, Deleting personal data after the ending of the legitimate term procedure* etc.
Based on the data received from the inventory the specific maximal terms for keeping the data is being determined., the procedures define how they are deleted/anonymized after the end of their keeping whereas the mapping of the streams determines which parts must be informed for the past terms (as well as for honored individual requests) so that they can take the needed actions.

5. Integrity and confidentiality

The idea is to be guaranteed suitable level of protection of the personal data through applying suitable technical and organizational measures. The aim is the personal data to be collected and processed in a way that the suitable level of security to be guaranteed including against unauthorized or unlawful processing and against accidental loss or damage.

The Company applies different technical decisions according to the specific of the collecting:

- On its websites:
    - Applying the principal of confidentiality be design according to which each new website or significant service are being analyzed for possible risks of breaking the confidentiality of the personal data (within their processing in question), arising form, the technology they use.
    - Regular actualization of the used software versions and full speed applying these actualizations when leaks in the used software have been found;
    - Specific checks of the ready code, e.g. SQL injections, vulnerability of XSS attacks, minimizing informative text in the messages about mistakes, validations on both sides – the client (browser) and the server, minimal obligatory requirements when generating passwords not only for the customers but also for the accesses to the administrative zones on the website/online product; specific checks when giving the chance for uploading client's files;
    - Using of HTTPS crypting protocol for the link between client and server and the protection of the communication between them;
    - Keeping the data for user access (passwords) in the data base in hashed appearance.;

6. Reporting

As personal data administrator **the Company** must develop procedures and to apply processes in such a way that makes it capable of proving keeping paragraph 1 from article 5 in accordance with the requirements of the same article.

According to the main vertical actions prove is needed in the following situations:

- Registration of new user profile in the website/online app. It is decided with the means of record in the specific for the concrete project data base containing timestamp of the operation:

    - Collecting personal data from employees. It is decided by dating all the documents containing the agreement of the employees for processing or changing their personal data;
    - Collecting personal data from trade partners. It is decided by describing all the personal data collected from them, dating the documents and the other ports of the collected personal data as well as creating and maintenance of a register of the collected personal data categories;
    - Personal data received by trader partners in terms of executing contract obligations. It is decided by describing:

    - Categories of the received personal data;
    - Categories agreements declared as received from the subjects of the trading partner;
    - Applicable to **the Company** restrictions when processing the personal data;
    - Terms for keeping the personal data.

Interested parties

The present policy is applied by:

- **The Company;**
- Employees on employment contract in **the Company;**
- Collaborators on civil contract in **the Company;**
- Sub executors, delivers, partners, consultants and third parties performing services for **the Company** and on behalf of **the Company** and receiving personal data or access to bases containing personal data. Executing the policy in this case is provided through adding suitable moral clauses selected on risk analysis base and through adding certain requirements and obligations towards the third parties – receivers of personal data for which **the Company** as Administrator or in specific cases – as Processor using the help of those third parties for executing the assignment.

The policy is valid for all the data which **the Compan**y collects, processes and keeps and which can lead to direct identification or to help identifying the individuals, for example:

- Name of individuals;
- Personal ID number of individuals;
- Data from the ID of individuals;
- Permanent and present addresses of individuals;
- Mobile and home numbers of individuals;
- Email addresses of individuals;
- Employment history;
- Bank account numbers of individuals;
- Records of work-related conversations led by employees of **the Company**;
- Video records of the offices of **the Company;**
- Online indentificators – IP addresses, device identificators, user identificators, website user's behavior operating by **the Company**, cookies and other ways for keeping the information and marking the users
- Specific identificators of the individuals in mobile apps such as:
    - IFA aka IDFA (Identifier for advertisers) – temporal identificator of the device of the user under the control of the last and compatible with mobile devices with operating system IOS
    - Google advertising ID – temporal identificator of user's device under the control of the last and compatible with mobile devices with operating system Android
    - Firebase Analytics – different events including containing personal data f the users of the mobile app ones

GDPR Roles

Each individual who is employee, consultant, sub executor, collaborator, or countSMBParts of **the Company** has responsibility for keeping the Regulation's requirement in terms of the lawful collecting, keeping and processing the personal data.

For the successful executing the tasks of keeping the security, protection and the confidentiality of the personal data the following key roles have been defined:

1. CEOs of the **Company**

   They guarantee sparing the necessary financial and human resources and supply the necessary focus and priorities of the employees for keeping the legitimate obligations of the **Company.**

2. GDPR officer - responsible for:

   2.1. Informing the CEOs in due time for responsibilities, duties, risks, issues and misses made in protection the personal data;

   2.2. Overview and approval of all the documents related to protection the personal data;

   2.3. Organizes initial and periodical briefings and trainings for the staff;

   2.4. Replies to questions related to the personal data protection made by individuals and other parties or competent persons;

   2.5. Processing requests from individuals for exercising their rights by the Regulation**;**

   2.6. Check and approval of contracts and related to them documents for collecting, processing, transfer of personal data;

3. Info security Manager - responsible for:

   3.1. Guarantees that the used systems, solutions, services and equipment used for collecting, processing and keeping personal data meets the standards of the industry for keeping their safety;

   3.2. Overviews and approves technical propositions for accepting new services;

   3.3. Takes part in the choosing of suppliers, related to the technical realization;

   3.4. Performs periodical and planned checks of the functioning, the state, the correspondence between the hardware and the software used in processing the personal data and keeping their security;

   3.5. Guarantees keeping the deadlines for depersonalizing, anonymizing and deleting personal data held in the SMBP of the Company in accordance with the approved policies;

4. Trade Officer – responsible for:

   4.1. Guarantees accordance of the job of his team in terms of the Regulation's requirements and the approved policies of **the Company;**

4.2. Performs initial briefing and periodical trainings of the employees of the team;

4.3. Creates recommendations for optimizing the work flow processes with the physical carriers of personal data;

4.4. Creates suitable organization for quick informing in case of a breach in the security of the personal data, object of labor of the Trading department;

4.5. Creates organization personal data holder's requests made by partners to the Trading department to be sent following the order described in the procedures and the policies. Such requests can be related to third party's data delivered as transfer related to the development of a new project for a Company's client;

4.6. Assures that the Clean desk policy is strictly followed by the employees in their team;

5. Chief Accountant – responsible for:

5.1. Guarantees that all documents related to the accounting operations of **the Company** meet the Regulation's requirements;

5.2. Follows for keeping the deadlines for depersonalizing, anonymizing and deleting the personal data in the documents by point 5.1 in accordance with the approved policies and keeping the applicable lawful deadlines and requirements;

5.3. Ensures the strict following of the Clean desk policy on behalf of the employees in the department;

6. Marketing director – responsible for:

6.1. Guarantees that the applied on websites/online products solutions working with personal data are in compliance with the Regulation's requirements;

6.2. Approves official statements on behalf of **the Company** related to collecting, processing and keeping the personal data;

6.3. Answers any questions in regards to the personal data protection;

6.4. Whenever needed works with other employees in order to secure the accordance of marketing initiatives and activities with the Regulation's requirements**;**

6.5. Performs initial briefing and periodical trainings of the employees in the department;

7. Financial director – responsible for:

7.1. Ensures correspondence of **the Company's** contracts with the Regulation's requirements**;**

7.2. Ensures strict following of the Clean desk policy by the employees of the department;

7.3. Performs initial briefing and periodical trainings for the employees of the department;

8. Work and Wage Director – responsible for:

8.1. Guarantees following the Regulation's requirements during the work flow of the employees of the department;

8.2. Performs initial briefing and periodical trainings of the employees of the department;

8.3. Must signalize immediately the GDPR officer in case of a breach in the security;

8.4. Forwards questions and requests form the personal data holders or third parties towards the GDPR officer;

8.5. Ensures strict following of the Clean desk policy by the employees of the department;

8.6. Is in charge and takes care for the physical storage and keeping the confidentiality of the files of the employees with employment, civil or copyright contracts;

8.7. Is responsible for the deleting or the anonymizing of the unnecessary personal data within the process of hiring such as received CVs;

8.8. Is responsible for keeping the deadlines for deleting or anonymizing of employees' personal data after the legitimate or negotiated period for their keeping has expired;

9. Internal Control Director – responsible:

9.1. Performs periodical, planned and unplanned checks of **the Company's** offices and teams aiming to determine the level of execution of the approved requirements in terms of keeping personal data;

9.2. Creates and gives reports and recommendations to the GDPR officer and the Team Leaders based on the noticed negligence and disadvantages;

9.3. Cooperates in employees' trainings;

9.4. Cooperates the GDPR officer for the normal execution of his functions;

10. Legal Councilor of **the Company** – responsible for:

10.1. Checking and concording of all legal texts;

10.2. Checking and concording of General terms, contracts;

10.3. Takes part along with the employees, performing other roles in analyzing projects different in terms of their legal compliance with the applicable legislation;

Risks which are related to personal data collection

The Company is identifying different risk in time, considering the possibilities that is not possible to identify all possible risks, otherwise there wouldn't be any possible risks

In order to minimize the risk possibilities, **the Company** analyses his main activities:

- Collecting, maintain and archive personal data for the people who are using company's websites;
- Collecting, maintain and archive personal data for the people company's online products;
- Collecting, maintain and archive personal data for company's employee;
- Collecting, maintain and archive personal data for any of the company's business partners;
- Database and corresponding functional code, where is located basically the system for managing business processes (SMBP);
- Database and corresponding functional code, where is located all the decisions developed by third parties;
- Personal data exchange with the office in Macedonia;
- Personal data transfer to **the Company's** partners

During the analysis the following points have been taken in consideration:

- Accidently or irregular data destroy
- Data loss
- Unauthorized changes
- Irregular data exposure or access to transferred, archived or other ways where personal data is maintained

All analysis outcome is available as documents for risk assessment and mitigation.

General Conditions

Collecting, processing, transferring and keeping personal data is only being done by individuals and if this is directly needed for performing their duties. These duties can result from job descriptions, employment contracts by the power of approved policies and procedures of implementation contracts.

Sharing personal data without valid reason is forbidden.

When in doubts whether a certain act related to personal data should be done or not the employee must ask the GDPR officer for cooperation.

The Company is obliged to perform initial briefing to all new employees and partners, consultants which is duly verified with protocol

An initial training will be performed for the present employees which will duly be verified with protocol

Periodical training will be organized for all employees during which different ways for optimization of the processes, policies, practices, approaches and documentation related to processing and keeping personal data will be discussed.

Access to procedures and policies related protection of the personal data

All internal procedures and policies defining the personal data protection in **the Company** are being kept electronically on the following address: \\data\Specifications\GDPR\Internal Polcy and Procedures

The document's content is confidential and all the documents are marked as *Confidential – for internal use only*. When working with the document's employees must not reveal their content outside **the Company**.

Access to information related to protection of personal data

Whenever access to digital or paper port carrying personal data is needed the employee must turn to their direct leader.

The personal data collected, processed and kept by **the Company** are preserved in the following places:

1. In **the Company's** SMBP database. The access is restricted by IP addresses and protected with user names and passwords. Employees performing certain functions within **the Company** have respectively restricted access to the data.
2. In the software storages of **the Company** because of the different projects including transfer of personal data by partners.
3. In the central office building of **the Company**.
4. In the office building of **the Company** in Republic of Macedonia.
5. In storages purposed for paper documentation outside of **the Company**.
6. In the storages purposed for e documents and code outside of **the Company**.
7. In the legal offices with which **the Company** has partnerships.
8. Within the partners in collecting data from websites/online products which are in EIP or in any of the countries from the list of the Countries and the International organizations for which decision for adequacy has been applied or in the list with organizations targeted in the Shield for confidentiality of personal life between EU and USA.

9. Within the partners providing industrially acknowledged decisions for hosting and equipment collecting.
10. Within partners giving useful solutions described in details in the List of Partners.

Measures for performing the employees' duties

Employees and individual giving services by the power of employment contracts must perform the following requirements:

1. To use secure passwords for access and not to dispose them to third parties.
2. Under no circumstances to share personal data outside the way which is described in the approved procedures and policies especially to external for **the Company** parties.
3. To strictly follow the Clean desk policy.
4. To have quickness of mind and clear judgment when determine the volume of the collected personal data as well as the way they should be transferred as far as this depends on their job description and de facto on the duties they perform.
5. To follow approved instructions, policies and guidance.
6. To lock their electronic devices when leaving them with no supervision.
7. All portable devices must be kept in a safe place when left with no supervision.
8. The internal communication within **the Company** to be performed only via work emails or any tool approved by the Management for internal communications.
9. Not to send any personal data outside the European Economic Zone boarder without the explicit agreement from the GDPR officer or without having a defined described process added as part of the procedures and the policies. If such need is present they must turn to the GDPR officer.
10. The use of PCs for keeping work related personal data without the explicit approval of the Information Security Manager is forbidden. The Information Security Manager gives such approval in accordance with the corresponded procedures when there are such requests.

Personal data in paper documents

Competent in regards to keeping the personal data are the GDPR officer and Information Security Manager. Any questions related to the ways of keeping personal data must be sent to them.

Although most of the data are being kept in electronic copies, the job specification implies using a lot of paper documents as well not only filled in by the users but also added to secondary documents created within the work process.

All paper documents containing personal data must be kept in a locked drawer at any time except when the employee has visual contact and direct control over the place where the personal data are being kept. Even in this case it's recommended that the personal data should be locked at any time when it's not being processed.

The movement of paper documents containing personal data is being done as per the order of the approved policy.

Employees must take care for the paper documents containing personal data not to fall into unauthorized hands and for this purpose they must not leave them on places where such thing could happen – printers, places outside **the Company**, places in the offices to which external parties have access.

After passing the deadline for keeping the data or when there is lack of need of a certain paper document it must be inevitably deleted by using the appropriate tool. (eraser).

The archived outside **the Company** personal data are being required in the same way by the archiving company and are being deleted in the same way and following the approved procedures.

For deleting data on paper carriers kept outside **the Company** it's recommended the process to supervised by a Committee in which its representatives participate and whenever this is not possible a protocol must be issued by the individual/firm which is responsible for deleting the personal data

Personal data in e-documents

Any data version is being protected on many levels according to its place of preserving

The servers on which SMBP is displayed respectively the bases with personal data is on hosting solution provided by entrusted supplier. The solution is behind a firewall and is being administrated by competent staff.

The data are being recorder in crypt mode in the base and the access to them is restricted by IP and by username and password. The passwords and the usernames must be generated in the same way which guarantees their complexity and reduces the chance of. Sharing passwords and usernames between the employees is strictly forbidden.

The access to the SMBP is secured through limited IP access usernames and passwords.

The personal data related to performing concrete projects are being kept safe in local web for developing projects. The rights for access of the employees are being controlled for each project, according to their work related duties in terms of the project and when needed relevant briefing is provided widening the work duties related to the concrete project and signing the relevant documents engaging the employees'

Part of the projects is being kept in distant software storages such as GitHub. When analyzing the risk anteceding such projects development where using such a solution is anticipated risk analysis has been made so that transferring personal data could be avoided.

When handing over such a project containing personal data to assignor personal data received by him are being used only in terms of performing the project.

When the data is being stored on portable devices (DVD, flash memory, external memory) the data must be kept locked when not in use. The place of the portable device must be known at any given moment

Transferring large amount of data is being done by the determined in the approved procedures ways only and towards the described in them parties. When transferring data in online environment a SSL crypting or similar technology is always applied for protecting the personal data.

Copies of the important data is being done regularly (back-up).

Adding unstructured data

SMBP allows adding unstructured data**.**

In order the risk of such collecting to be reduce it's recommended to the employees to be extra careful when adding unstructured data in SMBP

Employees are forbidden to create unnecessary copies of the data unauthorized process of the personal data adding metainformation creating own copies or massives containing data filter in any way.

Accuracy of the data

In accordance with the Regulation's requirements **the Company** must have developed policies and procedures for granting the opportunity for collecting as accurate data for the individuals as possible and also the individuals to be able to request correcting the data.

The Company understands how important it is to work with accurate and concrete data within its specific activities where this matter**.** For this purpose, when developing new online products or adding functionalities to the present ones the necessity of granting opportunities to the users to have access to their profile and the chance to correct and verify it (email address, sending verification email. Mobile number, sending PIN code for confirming address, by using cards from which the user selects the address etc.) has been taken in mind.

In addition to this each of the sites of **the Company** has Centre for Managing the Confidentiality as well in which the user holding personal data can take a look at his/her profile after logging in and make corrections to part of the data.

If inaccuracy of the data has been detected which cannot be changed in the profile the user can request to exercise his/hers right to correct the personal data which will be checked and executed within 30 days.

When assertive feedback is received that certain personal data are no longer valid they must be removed as fast as possible from SMBP and in the given deadlines for inventorisation of the personal data kept on a paper carrier.

Such examples are: email addresses, for which messages are being received that the email is no longer active or mobile numbers for is known that have a new owner.

Personal data inventorisation

The main aim of the inventorisation of personal data is to determine which of the personal data must be removed via depersonalizing, anonymizing or deleting depending on the appropriate context of keeping.

As additional aim possible correction of the personal data is being targeted.

Digital personal data

The inventory in SMBP is made once a year vial planned executing in unloaded business hour of number of logical actions in the base which end aim is to detect all information units in which there are personal data with expired period of keeping.

After such records have been found a number of measures are proceeded according to the situation:

1. Their depersonalizing – records are saved but the pe4rosnal data in them is being deleted. In this way the normal operation of the financial and accounting part of SMBP is guaranteed.
2. Their anonymizing- records are saved but the data in them are being replaced with values which stop the link of the data with the concrete subject. Such approach can be realized for unstructured data such as email communication and comments to the partner's profiles in the CRM system
3. Their deleting Some data categories such as those with marketing targets can be deleted after the expiring of the determined period and after its expiring they must be deleted.

For each performed operation regardless of its type a record is made containing indications that executing the operation is work process; indicator of the type of operation and timestamp counting the exact time for executing the operation. In this way conditions for accounting of **the Company** as an Administrator of personal data is being created.

Paper personal data

Inventorisation is being performed once a year and the requirements of the approved procedures are being followed. The personal data which have been found if fallen under the conditions for

deleting are being requested by the archive company or the office in Republic of Macedonia or are deleted in the central office.

The accounting firm/internal accounting takes responsibility to perform inventorisation of the paper data once a year as during that time specifies which personal data carriers must be destroyed. The peculiarity here is that the practical possibilities for depersonalizing and anonymizing do not exist.

Personal data individuals'requests for exercising their rights

Individuals holding personal data can use several channels for submitting their requests to **the Company**. This is described in details in the correspondent procedures.

The channels are:

1. Centre for Managing the confidentiality accessible from every site of **the Company**. User are required to login for identification security check.
2. Request form sent to **the Company's** address. Personal visit to the office is required for identity verification.
3. Employee form submitted in Human Resources department.
4. Re-sent request from a partner or client on behalf of the personal data holder and in line with transfer made beforehand from the client/partner towards **the Company**.

Special interface is being used where any taken action is displayed from entering to executing the request. For this purpose, employees who to be in charge have been hired and a procedure has been approved for processing the requests.

Disclosure of personal data due to special reasons

In certain situations, the Law requires personal data disclosure. Of the individuals without their agreement. Such cases are for example when judicial system has asked for such disclosure.

When such a request is submitted the GDPR officer makes a statement for each request for personal data disclosure and if needed consults with **the Company's** layers. And CEOs.

When the data are being disclosed the principals of minimizing the given data are being followed and of possible anonymizing of the data which is not necessary for the judicial system.

Transperancy and granting information

The Company takes care to ensure transparency of individuals holding personal data in regards with they being informed of the fact of their personal data being collected., the objectives of the process and the ways the individuals can exercise their rights

The individuals being informed is granted via especially added texts in the Individual's Agreement which antecedes collecting their personal data, signed agreements with employees of **the Company**, using templates in the contracts with counteragents.

Details on the matter can be found on each of the sites of **the Company** as well as in each of its offices.