1. General provisions

Cellact LTD is a communications and software company that specializes in providing business communications solutions, and is located in Kibbutz Shefayim, Israel.

Cellact LTD Personal Data Processing Policy describes the basic principles, objectives, conditions and methods for personal data processing, work procedures related to processing personal data, as well as requirements to the personal data protection.

The Policy is developed based on the requirements of the EU General Data Protection Regulation 2016/679 (the “GDPR”).

The Policy complies with the requirements of the Privacy Protection Regulations (Information Security) 2017 of the Privacy Protection Authority, Ministry of Justice in Israel.

This policy constitutes a commitment taken by Cellact to preserve the confidentiality of personal information of private customers, which are stored in its systems. Whether they are customers of the Company, who provide services to end customers, or whether they are end customers.

Cellact commits that access to these details will be given to authorized persons only and will be carried out only when necessary and with the consent of the customers.

Cellact undertakes not to transfer the details of the customers stored in its systems to a third party without the consent of the customers.

Cellact serves as a data controller since it determines the goals and manner of collecting, saving and using the data, and also as a data processor since it provides the means and implements the processing of customer data.

2. Definitions

i. The Company – in this document refers to Cellact LTD
ii. Cellact customer – a party that consumes products or uses services provided by the Company.
iii. End customer – a party who consumes products or uses services provided by the Company's customers via Cellact interfaces or infrastructure.
iv. The database - a database maintained by Cellact is a database with a basic level of security, according to the definition of privacy protection regulations. Cellact Company holds information for the purpose of contacting and providing service. Cellact does not collect information about the privacy of a person's personal life, medical information, genetic information, information about political opinions, past criminal information, communication data, biometric information, information about a person's assets, and consumer habits
v. Outsourcing / Third Party Vendor - A company that provides software / storage / integration services or other services to Cellact Company for the provision of services by Cellact to its customers
vi. Information security event - Damage to the integrity of the information as a result of hacking (external or internal) to the database, leakage of personal information from the company's database, use of / deletion of personal information in the database without satisfactory explanation, transfer of personal information from the database without authorization and other events that exist risk of exposing personal information from the database to unauthorized parties.
vii. User interface – web or phone applications manufactured by Cellact and are in use of Cellact's customers.
viii. Cellact infrastructure - Systems that allow sending SMS, email or voice messages to cellular, landline and email recipients, and other systems installed on servers located in two farms: a main site located on the Adgar farm in Rosh Ha'ayin, Israel; The backup site (DRP) is located in the Tamares farm in Tirat Hacarmel, Israel. The company's customers can interface with these software via an API or Web Service from external systems.
ix. Bigadmin management system - a system for internal use by Cellact employees, which enables management and control of the web interface used by the company's customers.

x. Mobile device - A computer designed for mobile use, including a mobile phone equipment device.

3. Purposes and applied methods of personal data processing

Cellact shall only collect, use or process Personal Data relating to Company's customers or end customers if the Processing falls within the scope of one (or more) of the legitimate Business Purposes listed below:

3.1. Providing service to Cellact's customers

Cellact provides its customers with infrastructure and applicative solutions for sending bulk SMS, email and voice messages, and other communications solutions. As a part of the service, Cellact maintains records and databases used by its customers.
In addition, Cellact provides its customers with the ability to generate reports on demand, through which Cellact and its customers can measure the quality and efficiency of the service.
The generated reports may also contain information about the Company's customers and end customers.

3.2. Receiving end-customer approval for sending marketing messages

As part of the Israeli Spam Law (2008), Cellact instructs its customers using Company's interface and infrastructure to send messages to end customers, that they must obtain written approval from the end customers for consent to receive marketing messages sent via SMS, email or VOICE messages.
The responsibility for receiving the approval, and for enforcing the Spam Law, is that of Cellact's customers towards the end customers.
However, Cellact provides guidance and solutions through which its customers can easily enforce the regulation:

- A clause in a contract with customers requiring them to obtain approval from the end customers for sending marketing messages
- Interfaces that enable blocking of end users who are not interested in continuing to receive the service.

3.3. Means of employee access to end customer information

3.3.1. Office Email

Accessing an office email box requires Active User permission on the AD

3.3.2. Reports interface

Enables Company customers to generate reports regarding messages sent to end customers.
Access to the interface requires customers user name, password and organization name from customers.
Cellact employees with appropriate authorization can access client reports via the Bigadmin management system.

3.3.3. DB servers, which hold the databases.

Enable privilege employee to run SQL for maintenance, tracing problems or as per customer specific request.

3.3.4. Access via mobile device

Some employees of the Development Department work by means of a mobile device that is encrypted and protected by a personal user name and password. The mobile device in question may contain information that is relevant to a development project on which the work is performed.

3.4. Use of Third Party Provider / Outsourcing by Select Company

Cellact may use third party / outsourcing services to provide service to its customers. A third party supplier may be an Israeli or international supplier (outside of Israel) through which services can be provided to Company's customers.
Before undertaking the contract / integration, Cellact will perform a risk assessment involving contracting with the supplier. The company will place the contract with the supplier at the level of these risks.
In the process of integration with the suppliers, verification is made that the information is not transferred to the supplier, which may lead to the identification of an actual person.
It should be noted that as of today, Cellact has no cooperation with third party suppliers / outsourcing, for which the company is required to provide information from the database that may lead to the identification of a real person.
In the future, should Cellact integrate with a third party supplier to whom personal information will be provided from the database. The Company undertakes to ensure that:

- Ensure that the vendor maintains privacy and information security procedures that comply with the regulatory requirements. Cellact also informs customers who use the service on the use of sub-vendor systems.
- If personal information of customers or end customers is transferred to a third party supplier, but the supplier does not have a privacy and information security policy that meets the regulatory requirements, Cellact will ask the vendor to sign a privacy and data security agreement. The agreement should specify

    - What information the supplier may process and for what purpose

- Which systems the vendor may access
- What type of information processing the supplier may perform
- What is the duration of the contract with the supplier and how will the information be returned to the owner at the end of the contract.
- A commitment by the supplier to maintain information security, including the signing of all the authorized access to Cellact database of confidentiality obligations.
- In the event that a third party provider permits access to the database for another entity for the purpose of providing the service, the details of the cause, the reason for the disclosure of the details, the purpose and manner of use shall be specified.

Communication with third party suppliers and control of information provided to suppliers, as well as formulation of a privacy agreement with the supplier - lies under the responsibility of the VP of Business Development.

- Select will notify customers using the service of using sub-vendor systems. Executive responsibility - VP Business Development.

4. Work procedures relating to Employee access and use of personal Data

4.1. Acceptance of new employees

4.1.1. Information security brief

In accordance with the Company's information security procedure, each new employee will undergo training in information security during the first week of work. As part of the training, the employee will be given information security principles, including:

- Use of personal passwords and confidentiality of passwords
- Prohibition of taking out of materials from the workplace, and prohibition of taking photos in the workplace
- Guidance for shredding printed materials
- Maintaining confidentiality of customer details in work process.
- Taking precautionary measures when sending sensitive information by e-mail Prohibition of receiving email from customers outside of the Cellact office network, except in an exceptional case and with the approval of the person in charge of information security.

4.1.2. Signature of confidentiality agreement

Each new employee will sign a confidentiality agreement with Cellact. Under the agreement, it is forbidden to issue any information related to Cellact systems or customers, or to forward them to a third party.

4.2. Employee access to customers' personal information.

4.2.1. Organizational Structure

The number of employees in the company (number of people with access to the database) is about 40-60 employees.

- CEO
  - Projects and development
  - Operations and delivery –
    - Operations
    - IT
    - QA
  - Service management
    - Tech support
    - CR
    - Service
  - Sales
  - Finance
  - HR
  - Tydo telecom Sales and CR staff

4.2.2. List of all roles with access to systems holding personal data

Role	Access level
Tydo Telecom Sales and CR team	Email access The team does not have administrative access to Bigadmin. If needed, they request access details to customers interface from Cellact Tech support and access it directly.
Service	Email access Bigadmin management system with access to reports
CR	Email access Bigadmin management system with access to reports
Tech support	Email access

	Bigadmin management system with extended access Access to MySQL DB and operational logs
Operations	Email access Bigadmin management system with extended access Access to DB and operational logs and Billing Access to data stored on operational servers.
IT	Bigadmin management system with extended access Access to MySQL DB and operational logs Access to FW, SW, Servers and storage
QA& Development	Bigadmin management system with extended access Access to DB and operational logs and Billing Access to data stored on operational servers.

4.2.3. Cases in which the customers data will be accessed.

Customers' data will be accessed by Cellact staff only on need to know basis.

4.2.3.1. CR will access customers' data at the customer's request to produce a report, to assist in the operation of the system or to transfer a request for treatment to one of the other departments in the Company.

4.2.3.2. Service is the department that assists the Company's customers in producing campaigns for end customers, and performing various operations in the interface such as blocking recipients or generating reports.

They will access customer details in the system only at the customer's request to perform one of these operations.

4.2.3.3. Technical support will access the system at the request of a customer for assistance in performing actions in the system, or in order to treat a problem reported by the customer.

In addition, technical support will produce statistics according to the management's requirements for conducting customer satisfaction surveys and internal use of the Company.

4.2.3.4. Operations will access the systems as a second support line in case of malfunctions or customer inquiries.

Operations, IT, Development and QA will only access the systems in the event of maintenance or updating of the system version.

4.3. Employee role change procedure

When changing the role of an employee, the employee's permissions will be updated according to his position. An employee who has moved to a position with lower privileges will not have access to systems that are not necessary to perform his function, even if he has had access in the past.
This is done by changing the employee's affiliation to email groups, and changing the IP address of a workstation and AD rules.

4.4. Job termination procedure

At the end of a working period, all the user permissions of an employee are revoked, including:

- Access to work station by deactivating user in AD
- Remote access to the office via VPN in the FW
- Closing the personal email box

4.5. Customer identification and submission of information

In the case of a customer request to receive or change details in the interface, Cellact representatives will make sure that the request is recieved by e-mail, and that the sender's mail belongs to an authorized contact.

Interface access information should never be delivered by phone. It will always be sent to customers by email or SMS to an email address / telephone number updated on the systems as contact details.

Information for contacts that do not appear as authorized contacts will only be provided after receiving a confirmation email from an authorized contact in the customer's account.

4.6. Generating and sending data reports to customers

Cellact representatives will send reports to the Company's customers at their request. Reports must be sent by email only to addresses approved by authorized contacts.

5. Security measures for controlling access to personal data

Cellact shall take appropriate steps to protect customers' and end customers' personal data from unauthorized access and other unwanted or unlawful processing.

5.1. Office Firewall

Prevents access to the Company's systems outside the office.
Connect Production environment by VPN Site-2-Site.

5.2. Active directory

Defines and manages access rules for systems.
Each user has personal and unique access details for a work station.
Password restrictions are detailed in Appendix A (separate document).

5.3. mEnterprise Bigadmin management system

Available only from within office Firewall.

5.4. Employee remote connection to office

Is performed through a VPN connection with a user identification mechanism using access information and an access code sent to the employee by SMS.
The authorizations of connection to the office are managed by AD.

5.5. Physical security of the company's equipment on which the database is located

5.5.1. Means of security for physical access to information at the Company's offices

- Entry to the company is through a personal card / chip for each employee
- The company has electronic security measures (cameras)
- Existence of a procedure for entry of visitors into the Company's office (customers, suppliers): the obligation to meeting and continuous accompaniment of an external person until he leaves the office.
- The procedure for locking personal computers of employees during breaks.

5.5.2. Security measures for physical access to a server farm where the company's database is maintained

- Adgar Farm
- Any person who comes to the farm must be on the list of authorized persons and obtain the prior approval of Cellact's information security officer coordinated with technician at the farm on arrival and access to the company's servers.
- At the entrance to the farm, all visitors are photographed
- At the entrance to the farm area, the visitor's biometric identification is performed
- The visitor to the farm is accompanied at all times by the farm technician
- The server cabinet is locked at all times and is opened by a farm technician only. The technician keeps the key to the closet.

- Tamares Farm
- The visit of the company employee to the farm requires the prior approval of the information security officer coordinated with farm manager on the day of arrival.
- Face photography of the farm visitor.
- Accompanying technician while visiting the farm

6. Resource asset management

6.1. List of IT equipment in Appendix B (separate document).

6.2. Work stations in Appendix C (separate document).

6.3. Update IT equipment procedure

If new equipment is purchased, or if a version of systems is upgraded, the new equipment model or version information will be recorded and updated in a privacy policy document.

7. Privacy Policy for Cellact website visitors

i. This document is an integral part of the **Site Terms of Use** document.

ii. The company respects the privacy of every person who visits the site. The privacy policy described below refers to the type of information that the Company may collect, as well as the way and purpose of processing this information. This policy of the company also instructs and guides visitors how to act in case they do not wish their personal details to be collected or delivered to others in connection with their visit to the site.

iii. The Company manages a database and may process any information about its subscribers or users of the Site (such as name, address, telephone number, e-mail address, etc.) (hereinafter: "**Personal Information**" or "**Personal details**") which will become known as a result of using the Site and / or transferred by users / subscribers of their own free will..

iv. The Company undertakes that the use of the personal information and the manner in which it is managed will be for any purpose within the Company's business activity and in accordance with the provisions of the laws of the State of Israel applicable to that matter.

v. If a non-subscriber, (i.e. a user who does not have a user account on the Site) does not wish their personal information to be collected, stored or processed in any way as described above, it must refrain from transferring its personal information to the company.

vi. It is hereby clarified that for providing personal information by a person under the age of 18, the consent of a parent or guardian is required.

vii. A user of the site who has consented to the conditions described above regarding the collection, storage and processing of his personal information in accordance with these provisions may exercise any right reserved to him under the privacy laws of Israel. A user of the site who wishes to exercise his right as aforesaid shall do so by means of a written request or an e-mail to the Company at info@cellact.co.il.

viii. The Company shall have no liability in the event that the Site User transfers or informs the Company or a third party, whether in the services of the Site or its contents or voluntarily, the personal details of another person (including without limitation, name, address, e-mail address, telephone number, etc.) That the user of the site first received the consent of that person. In such case, this notice will be made at the user's sole responsibility.

ix. Please, note that by creating the username on the Site and / or becoming a subscriber of the Company, you agree that the Company may contact you in any media that it deems appropriate in various advertising offers and messages relating to the Company's services. If you are not interested in receiving these messages, please contact us by email at info@cellact.co.il or by phone: 09-9704100.

8. Data privacy in Cellact products and applications

Cellact Privacy Policy is designed to allow users to understand what information is collected and how this information is used to ensure good privacy and security protection for users.

Cellact provides a range of products that include information that customers upload to send messages, establish phone calls, send emails or receive faxes.

In any use of Cellact Software or Product, different information is collected according to the nature of the product. We explain what information we store and collect about the different products and how we use them.

8.1. General

The information we collect includes:

Information that comes directly from the user it provides to the system. This information includes personal information such as name, email address, phone number or cases of receiving payment from businesses - also credit card details.

8.2. MEnterprise, integration with ME API, ME WS and sending automated campaigns via FTP

The infrastructure enables the company's customers to send SMS, email and voice messages to end customers, as well as receive alerts and answers from end users via SMS, redialing or clicking a link within SMS or email messages.

As part of the service, Cellact systems are exposed to the following:

• Telephone numbers and e-mail addresses of end customers and their affiliation to the distribution lists of the Company's customers.

• Content of SMS messages and voice messages sent to end customers via Cellact infrastructure and SMS message content sent by end customers to the Cellact virtual numbers available to Company customers.

• Content of email templates sent to end customers.

Data is saved on several levels:

• System Logs - The data is stored for a limited period of up to several days, and is used to solve technical issues.

• DB and Report Interface - The data is used by the Company's customers for viewing statistics and sending data, and for details received from end customers. By default, outgoing message content is not saved in the DB and Reports interface, except at the client request.

• System CDR files - the data serves as the basis for a periodic billing mechanism for customers. The information in the CDR files may be used for investigation in case of malfunctions. Message content is saved by default at the CDR file level for technical investigation if required, as well as in case of claims or court order.

8.2.1. mEnterprise interface

The mEnterprise system is one of the systems used by Large Account customers to send SMS, email and voice messages.

The settings include customers interfacing with ME API, ME WS, and automated campaign submissions by transferring files to FTP, SFTP, or safes.

In addition to what is written in Section 8.2, customer information stored in the systems also includes files that the user uploads to the system via a web interface or FTP or SFTP file transfer, such as distribution lists for distributing text or voice messages, and updating user information in mailing lists.

These lists may contain end-user personal information such as phone numbers, email addresses, first and last name, address, and other personal information that the user chooses to upload to the system.

The information is used to send messages to end customers, where personal information is used as part of the message content, as well as for the generating reports and statistics by the company's customers.

Managing, updating and deleting mailing lists is the responsibility of the Company's customers. Access and updating of the lists, including their deletion, by representatives of the Company shall be made only at the request of the Company's customer.

8.3.Cellact Communications services

8.3.1. Cellact SIM

Cellact Communications provides its customers with SIM cards and serves as a mobile operator.

Data stored in Cellact Communications systems regarding SIM card uses are:

• Details of the customer who purchased the SIM from Cellact, whether it is a private, business or White Label customer, for distribution use.

These details include: full name, company name, company ID, billing address, email address, telephone and billing details. The details are stored for billing the customer and in order to maintain contact with the customer and identify him when contacting the company call center. For sending an invoice and producing data according to the customer's request.

Cellact Communications does not store the details of those who purchased a SIM card from a White Label client

• Details of SIM usage. Details include the selected MSISDN number, date and time of use (call, SMS, DATA), originating / receiving MSISDN number, call duration and call status.

The data is stored in the systems for the purpose of periodic billing of customers, generating reports for customers on demand and for technical investigation in cases of malfunctions. In addition, data will be provided in case of court order.

Option to record calls to SIM customers - The option will be set only at customer request. Cellact Communications does not store the recording files: the files are deleted from the systems after they are sent to the client.

8.3.2. Voice services – stars, SIP connections, call routers and ATS services

Cellact Communications provides its customers with mobile / landline virtual numbers on the Cellact network, as well as short number services (asterisk) used to generate and receive calls.

Data stored in Cellact Communications systems in connection with the use of VOICE services:

• Details of the customer who purchased the service: full name, company name, company ID, billing address, email, telephone and billing details. The details are stored for billing and

maintaining contact with the customer, and for the purpose of sending an invoice and producing data according to the customer's request.

• Voice services usage details: Details include the Cellact Communications MSISDN number ("shadow number"), the short number (asterisk) in the case of the star service, the number originated / received the call, routing information (MSISDN number on clients side / customers ATS number), status, and call duration.

The data is stored in the systems for the purpose of periodic billing of customers, generating reports for customers on demand and for technical investigation in cases of malfunctions. In addition, data will be provided in case of court order

8.4. The SecNum app (Num2)

The secondary number / Num2 application allows you to use an additional phone number on an existing device without having to purchase a SIM card.

i. The Num2 application does not collect information from the device's Contacts list and does not use it except for dialing a contact or identifying an incoming call from Contacts.

ii. Permissions that are required to set up in the app installation:

• In-app purchases - You can purchase additional in-app services.

• Device and app history - The app can read within the call log and find the call records made to the secondary number.
• Contacts - The app can use your device's contacts, as well as create and change a temporary contact for the app, to show caller ID.
• SMS - Read the text messages sent to the app from a special app-related identifier
• Phone - The app can use your phone and / or call history. Phone access may include the following capabilities:

o Direct call to phone numbers

o Write a call log (for example: call history)

o Reading a call log

• Pictures / Media / Files-To set up a ringtone in a call / SMS

• Info on calls - The application can access information about all call participants, including the MSISDN number associated with the device on which the application is installed, and an MSISDN number of additional participants in the call.

iii. Information gained from application use, such as history of user actions, IP address, cookie, or information about the model of the device from which the user is using web, the cellular network from which the user arrives, this for secondary number app usage only. This information includes info how to use the Cellact services, the phone number to which a message was sent, or a message received, call log, call duration, date and time. Information for the investigation in case the application crashes, which includes operating system information and application identification, the browser, language, and the date and time of the crash.
App information such as a unique number that is installed for each application.

We store local information on the end device such as an application's private phone book, message and call logging, or application status such as Call forwarding, Call barring, or Voice answer forwarding. In addition, a call forwarding address is stored.

We record calls according to the customer's request and send them to the destination according to the customer's choice. We do not store the recordings in our systems after they are sent.

We keep the user's real phone number and the numbers assigned to him by the various services in order to know how to associate them with the user.

8.5. Mobile manager app

The Mobile Manager application enables the customer to manage a virtual switchboard for a business controlled by the cellular device and uses various cellular or stationary devices as extensions. You can ring a group of numbers.

i. The Mobile Manager application does not collect information from the device's Contacts list and does not use it except to dial through contacts or identify an incoming call from Contacts.

ii. Permissions that are required to set up in the app installation:
• Dialer access - to enable dial-up transfer to a set of numbers defined under the switchboard.
• Contacts - The app can use your device's contacts for app settings. Contact information is stored locally on the device and not transferred to the server.
• Receive SMS - Read text messages during application registration only.
• Phone - The app can use your phone. Phone access may include the following capabilities:
o Direct call to phone numbers

• Full access to the Internet - application work is based on the use of browsing data to allow access to the application server to access settings and routing calls and SMS according to the settings; Also to view and edit additional numbers defined under Num2 tab.

iii. Information gained from the use of the system, such as logs of user actions, IP address, cookie, or information about the model of the device from which the user is surfing, the cellular network from which the user arrives, for use only in a Mobile Manager application. This information includes usage character of Cellact services, the phone number to which a message was sent or received, logging calls including the duration and date and time. Information for the investigation when the application crashes, which includes operating system information and application identification, the browser, language, and the date and time of the crash.
Information of app usage such as a unique number that can be installed for each application.
We store local information on the end device such as call logs, and a call forwarding email address .
We record calls according to the customer's request and send them to the destination of customer's choice. The proper arrival of the recording file in an email to an end user depends on a number of factors, including correct email address, e-mail server and end device health when sending the file, and other factors independent of Cellact systems. As a result, Cellact does not guarantee that email containing call recording will be properly delivered to the user's email box. We do not store the recordings in our systems after they have been sent, so we can not retrieve a recording if it has not reached a user's email or was deleted by the user.
We keep the user's real phone number and the numbers assigned to him in the various services in order to know how to associate them with the user

8.6. How do we use the information?

The information that we collect and receive is intended to enable the service for users. We may use the user's phone number or email address to contact it for technical or other questions that arise in the use of our services.

We use the distribution files that the user uploads to make it possible for the user to send text messages, mail or calls to destinations at times chosen by the user.

We use data to provide user reports about the use of our services.

We keep the real phone number of the user and the numbers we assign to him in the application to enable the various services of call transfer and referral.

It should be noted that calls and messages sent by the user reach different destinations of his choice and attention should be paid to the issue of the privacy of the information when transferring this information to others.

Saved information includes regulatory instructions that must be kept such as details of calls and messages and assigning a number to the user.

8.7. Does Cellact share information with other companies?

Cellact shares information with Cellact Communications on the provision of its services to users. Information sharing is for providing service and continuity of service.

We do not forward information to third parties or other companies.

We are subject to the laws of the state and the regulation and transfer information to the parties following a legal demand in which there is a demand or request for information such as a judge's order to reveal a telephone number or call details. We will allow access to information for investigation on suspicion of fraud or any violation of state law. We will allow access to information in the event of security issues or technical issues

8.8. Information security measures in Cellact products

For security purposes we use SSL certificates to encrypt traffic between the user and the system. There is a possibility of choosing the client for certain services not to use SSL encryption for various reasons - and then one must know that the traffic between the user and the system will be exposed on the network.

We use physical systems and software systems to protect information and prevent unauthorized parties from reaching it. We provide access to information to authorized employees under a confidentiality agreement to which they are bound.

9. Information security risks and handling of information security events

Cellact Company has set itself the goal of identifying the main risks of jeopardizing information security in the Company and preparing to prevent these risks by means of appropriate information security measures and work procedures.

9.1. Possible information security risks

- Exposing information to a person who is not authorized by an employee due to human error or intentionally.
- Granting access to external factors by Cellact employee due to non-performance of procedures, human error or intent.

- Web Service services that are open to the world in an old, out-of-date version may be the target of hacking by malicious elements.
- Exposing employee workstations to security breach following receipt and opening of phishing email.

9.2. Ways of thwarting these risks

- Definition of work procedures for access and use of data, and procedures for identification, authorization and delivery of information to Company customers (section 4)
- Defining security measures to control access to the database (section 5)
- Regular updating of hardware equipment and security software for the updated versions (Section 6)
- Updating procedures and regular control over the enforcement of information security procedures in the Company.

9.3. Regular control over the execution of procedures and compliance with the requirements of the regulations

The information security officer regularly performs information security audits (both overt and covert) to examine and identify employees' data security exceptions. In addition, the Company's systems have automated testing and monitoring, whose function is to locate and warn of unusual activity or possible breach.
Monitoring data, and access information, authorization management info are kept in Cellact systems for a period of 24 months at least (most of the registration is kept indefinitely).

9.4. Handling an information security event

9.4.1. Identifying information security event

An information security event will be identified by one of the following measures:

- Automated monitoring systems: WAF, AV, IPS, and IDS that block unauthorized access attempts and alert the IT department.
- Data leakage blocking system DLP - blocks attempts to transfer information from personal computers to a USB flash drive, and alerts the IT department.
- Department managers regularly monitor email content sent by service and support representatives, and account managers to detect and prevent unsolicited information from being sent.
- Customer complaint

9.4.2. Handling an information security event

In case of possibility that a security event took place, an in-depth investigation of the event will be conducted by the relevant parties in the case in question: department managers, technical teams, the IT department, as well as automated means such as monitoring and recording systems.

After the event is investigated, a summary email will be sent by the responsible person (IT team, department manager, information security officer, or vice president of business development), including case study, event cause analysis and implementation conclusions to prevent recurrence.

9.4.3. Documentation of information security event

Documentation of information security events is the responsibility of the information security officer / IT department, or in the event that information is disclosed by representatives of service teams to unauthorized parties - under the responsibility of the VP of Business Development.

10. Delivering Cellact LTD Personal Data Processing Policy to employees

All Company employees must be familiar with the Privacy Policy.
All Company employees will be briefed on the main issues of the policy, and procedures through which they are implemented.
List of employees who underwent training regarding GDPR policy in Appendix D.

10.1. Annual update of the Company's information security procedure

Once a year, an information security policy and information security procedure are audited and updated, including all its appendices (list of IT equipment, list of workstations, instructions for managing AD passwords, list of employees who have been trained in information security and privacy policy).
During the evaluation, the following aspects are examined:

- If material changes were made to the Company's systems that hold the database, or to information processing processes
- If new technological risks relating to the Company's systems are known.

Responsibility for implementation: person in charge of maintaining and enforcing regulatory

11. Responsibilities

The Company shall appoint an employee who is responsible for maintaining and enforcing the GDPR regulation policy. The policy enforcement officer should ensure

that policy is passed on to all employees. He must ensure that all Company's personnel carries out its principles and instructions, as well as the implementation of the principles of the policy in all relevant work processes.

o In charge of maintaining and enforcing regulatory policy - Anna Arow
o Information Security Officer - Hagai Shporer

12. Contact us

For any questions regarding this privacy policy, please contact the company by:
Phone: +9729-9704100
Email: info@cellact.com
Fax: +9729-9704168

Written by: Anna Arow	**Role: PM**
Updated by: Hagai Shporer	**Role: OM**
Approved by: Amir Dorot	**Role: CEO**