JobCTRL®

JC360

INFORMATION SECURITY DOCUMENTATION FRAMEWORK

FOR THE COMPLIANCE OF REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

issue date: April, 2018.
issued by: Chief Information Security Officer

date of last revision: August, 2019.
version: 2.0

Executive summary

EXECUTIVE SUMMARY

JobCTRL Ltd is committed to fully comply with the highest information security standards and requirements. We are also committed to help our customers fulfill all relevant requirements as Datacollector using JC360 service and its related tools. Therefore we prepared this documentation framework to support compliance with GDPR specific requirements.

These documents may be enough for basic usage of JC360 client and server environment, however the framework documents are available in DOC format for further customization.

The JC360 configuration, access management and features enables additional customization options to ensure that JC360 data collection are fully in line with the Datacollectors goals.

Our information security experts are ready to answer any security related question in 7/24 at security@jobctrl.com.

25 May 2018

Ferenc Perjés

Managing director

Table of contents

DATA PROTECTION POLICY

1. Regarding the activity performed based on the Contract, Service Provider (JobCTRL Informatikai Kft.; 1118 Budapest, Rétköz u. 7.; company registration number: 01-09-949636; represented by: Ferenc Perjés managing director; phone: +36 1 465 8808; e-mail: support@jobctrl.com is considered as processor, Client is considered as controller.

2. Purpose of processing during the provision of the service: Analysing and developing business efficiency of Client

3. To this end, Client applies key performance indicators (KPI) that requires transparent workflow and provides an opportunity to improve work processes, make them more efficient thus enhancing effectiveness. These indicators are created via the aggregation of the key data generated during the work. The measurement of the key data required for the improvement of business efficiency is carried out using the software elements of the Service. While doing so, Client asks related employees to set JobCTRL applications in work status when performing the work set out in their employment contract which forms part of the analysis and improvement of efficiency, thus enabling the collection of key data for statistical purposes.

4. JobCTRL client performs central data collection exclusively in Work status (Internet addresses (URLs), window captions, e-mails, document names and paths, mobile coordinates, phone numbers, other specifically collected data) about which information is provided to the persons performing the work when installing the client software and during usage. Clients indicate this information in a text format, with icons and colours as well.

5. Employees can switch off the work status any time, and they can even set automatic rules for this purpose as they wish. There is an option to set central rules, that log out employees from the work status under certain conditions (e.g. when the system is evidently used for private purposes).

6. Similarly, under certain conditions (e.g. when the system is evidently used for work), there is an option to set entry rules. When the relevant conditions are met, the client automatically switches to Work status. In such cases the client informs the user about the changing the status using colours and icons. These rules can be set by the employee or Client's administrator centrally.

7. Based on the operational concept specified above, only work-related key data defined in accordance with the purpose of data collection for the analysis of efficiency and development and required for the aggregation of KPIs are collected. Employees can view these data any time (in the client, and in the Reports menu / Dynamic workflow report), modify or erase them (both in the client and on the website). Thus, the Service provides

comprehensive opportunity for self-determination regarding the key data. To ensure the reliability of the measurement, the certain modifications and manual data recording is indicated as “Manual data modification”.

8. Key data related to the work can be deleted from the system (in a time window to be set by the user in the client and on the website at organisational level, and also centrally and automatically based on various sets of Administrator data and for optional periods). In addition, usage for statistical purposes can be ensured without personalization via depersonalization (by rewriting the name and e-mail address of the user).

9. Service Provider provides all necessary assistance to Client to ensure the minimum amount of key data required for Client’s business purposes and provide the most efficient analysis (data minimisation). When launching the system, the default setting is the data collection specified in the Contract.

10. Service Provider makes every effort to comply with the highest professional and legislative requirements. Accordingly, the ISO27001 certification is maintained and Service Provider submits to the relevant professional audits on a yearly basis.

11. Service Provider is entitled and obliged to store and process the work data of the Users included in the database according to the instructions of the Client.

12. Service Provider undertakes not to use the data collected for purposes other than the one specified above. Service Provider may not create a copy of such data in any way except for the backup copy required for normal operation of the Service.

13. Service Provider undertakes not to disclose the data acquired during the performance of the Contract to any third party.

Annexes:

Annex No. 1 Relevant context of processing In accordance with the requirements of Article 13 of the GDPR

25 May 2018

Ferenc Perjés

Managing director

Annex No. 1 Relevant context of processing In accordance with the requirements of Article 13 of the GDPR

We draw the attention of controllers to the need to define more precisely each processing circumstance, such as:

If the controller has appointed a data protection officer, they shall also indicate their contact information in the Privacy Policy.

If the controller specifies the purpose of the processing, then obviously the information must be reflected in the Privacy Policy.

If the controller defines more clearly the legitimate interest in using the JC360 service, then this should be included in the Privacy Policy.

If the controller uses the JC360 to decide which measurements to set, they are aware of what personal data is covered by the processing and needs to adjust the scope of the data to suit their actual practice.

The duration of processing should also be specified by the controller, the general wording (what is the default setting) does not give a clear answer as to how long the data will actually be stored.

Name of controller:	Client as controller
Contact details of the data protection officer, if any:	Contact persons appointed by Client
Purpose of processing:	The purpose of processing is to improve organizational efficiency. Data management is only and exclusively related to the business data generated during the work.
Legal basis for processing:	The legal basis for processing is Article 6 (1) (f) of the GDPR, the legitimate interest of the employer.

Scope of data processed:	Data collection related to JC360 service IT support is performed only in an on and off state. Data collection related to JC360 service IT support can be controlled (enabled / disabled) at an organizational / group / employee level. The following list describes the full set of options that may be different (less) from the custom organizational setting. The JC360 PC Client can record the following data in working (green) state: Job task selected in JC360 ("Job" by default, but this can be expanded and changed with rules, eg change to "SAP use" task in SAP.exe) The name of the active application (eg explorer.exe) and address bar The value of the URL field Űin the active window of supported browsers (Internet Explorer, Chrome, Mozilla Firefox) In the supported mail client (Outlook, corporate Gmail, Lotus Notes), the From, Email, Subject, fields For supported office applications (Microsoft Office, Acrobat Reader), name and path of the opened document Computer Usage Intensity Indicator (number of mouse and key activity per minute based on real activity) 30 second sampling of on-screen app images (blurry levels: good / medium / bad / censored) - off by default Individual processing points (eg contract ID, customer ID) if required by the controller The JC360 Mobile Client can record the following data in working (green) state: Job task selected in the JC360 mobile application ("Job" by default, but this can be expanded and changed with rules, eg change to "Mail" task in email application) GPS positions Non-private phone numbers (caller / called) and call duration

	Name of active applications Photos taken manually with the mobile device from the JC360 mobile app with attached notes. Note that can be freely edited or selected from a predefined hierarchical structure, Individual processing points if required by the controller (eg POI name is stored for GPS based POI determination)
Profiling:	Pursuant to Article 13 (2) (f) of the GDPR, the logic of profiling and its impact on the employee should also be addressed in the Privacy Policy. The description in the previous section of the Privacy Policy, under the topic of managed data, also properly illustrates the logic of profiling. Adding to this is that subjects have access to the data processed by the JC360 service, giving them a better understanding of how processing works. The JC360 service has no direct consequence / impact on employment, nor may it directly place the employee at a disadvantage due to JC360 data and analysis. However, the data and results measured by the JC360 and visible to the employee may be part of the employer's evaluation process and may be used in it, but this is described by the employer in other policies / description of procedures.
Duration of data management:	Collected data is stored by default in the system for 5 years, but can be individually configured at the organizational / group / employee level (in days). The storage period is calculated from the moment of collection, after that, the data is permanently deleted.
Information on the use of a processor:	Information of the processor used by the controller: JobCTRL Informatikai Kft. (1118 Budapest, Rétköz st. 7.; registration number: 01-09-949636; represented by: Ferenc Perjés director; telephone: +36 1 465 8808; e-mail: support@jobctrl.com)

	In performing data-processing activities, processor designates the following subcontractors as potential contributors: TcT Hungary Kft. (1118 Budapest, Rétköz utca 7.; registration number: 01-09-937541; represented by: Attila Vadász) INPHONE Kft. (1118 Budapest, Rétköz utca 7.; registration number: 01-09-562494, represented by: Zoltán Baradlai) JobCTRL performs the following personal data activities for the controller: configure and fine-tune the system and service according to the objectives of the controller, understanding and evaluating business processes, creating, fine-tuning, benchmarking business performance indicators (KPIs), preparing individual analyzes, reports, examining differences, if required or claimed.
Persons authorized to access the data:	The collected data is stored in a closed system. Access to the data can be controlled by the controller / Employee / Team Leader / Admin authority and can only be accessed through authorized target reports. Admin controls the admission of target reports, which can be waived by other Admin users. Target reports can be enabled / disabled at the organization / group / employee level. The employees can see all data about themselves in the authorized target reports. The team leaders can see the details of themselves and their assigned employees in their authorized target reports. Admin can see everyone's data in their authorized target reports.
Information on data security measures:	The controller and the processor shall treat the stored data in accordance with the highest professional standards. The processor is ISO27001 certified and complies with the relevant sections of the GDPR Regulation.

Rights and remedies of the subjects of processing:	Subjects may first issue their complaint to their immediate supervisor or the head of the controller. Supervisor authority: National Authority for Data Protection and Freedom of Information (1125 Budapest, Szilágyi Erzsébet fasor 22/C). The rights of the subjects are as follows: Right of access: Based on the GDPR, an employee may request information about processing in connection with them. In this case, the controller (employer) informs the employee about what personal data is processed about them, for what purpose, the duration of the processing, the rights related to processing and the right to file a complaint to National Authority for Data Protection and Freedom of Information. The employee may request a copy of the personal data managed by the controller. In addition, it is worth noting here that the employee is able to see the data collected by the JC360 service within their own account. Right to Rectification: Although the employee may modify the data collected by the JC360 service within the specified limits, the GDPR provides the opportunity for the employee to request the controller to modify any personal data. Right to erasure: although an employee may delete certain data collected by the JC360 service within the specified limits, the GDPR provides an option for the employee to request the controller to delete some personal data. Right to restrict processing if the personal data collected by the JC360 service is inaccurate and up-to-date according to the data subject, the controller must suspend processing for the period of time that it verifies the accuracy of the data. If processing is unlawful (for example, National Authority for Data Protection and Freedom of Information has determined this) and the data subject objects to the deletion of personal data, the data subject is entitled to request that the data collected by the JC360 service be restricted. If the manager no longer needs the data collected by the JC360 service, but the data subject requires it to present, assert or defend legal claims. If the data subject objects to the controller (employer) employing the JC360 in connection with the controller, the controller shall suspend the data collection for this employee for a period of time that he or she

	investigates whether the arguments raised by the employee override the the legitimate interests of the manager. Right to object: the employee shall have the right to object at any time to processing related to the JC360 service for reasons related to his or her situation. The controller then examines the arguments put forward by the employee, ie whether the arguments raised by the employee override the legitimate interests of the controller.
Processing based on legitimate interest:	Measuring, analyzing and improving organizational efficiency is an inevitable element for market players in our industry. We have done processing so far and our evaluation system was based on them. This processing only makes our measurements and analyzing more complete, accurate and up-to-date, so we can design, develop and process them in a more focused and efficient manner. The range of data collected can be controlled. In accordance with the principle of data saving, only the data required for the purposes of the targeted reports will be stored for each data subject, and only as long as they are required. Data is basically used in target reports where we display aggregate business metrics (KPIs).

DATA PROTECTION IMPACT ASSESSMENT

Table of contents

This DPIA is created using a software named "PIA" developed by the by the French Data Protection Authority (CNIL). It meant to guide the data controllers in building and demonstrating compliance to the GDPR. It helps to properly carry out a data protection impact assessment by facilitating the use of the PIA method developed by the CNIL.

The current content may need customization in some cases. The content is available in the DPIA software internal JSON format as well, you can request it at support@jobctrl.com

DPIA-INFORMATION

DPIA
JC360

Author
Dr. Tamás Forgács, CISA, CISM

Reviewed by
Dr. Tamás Forgács, CISA, CISM

Approved by
Dr. Tamás Forgács, CISA, CISM

Creation date
23/03/2019

SUMMARY

Overview

A brief introduction of data management

The Data Manager is the JC360 service running organization itself.

The Data Manager is active in the service sector. Data management is primarily done for positions that work on information technology (computer and mobile) devices and the effectiveness of their work requires further development based on market expectations. As a result of data management, we expect to shorten lead times, improve quality in these jobs, and to automate each subtask.

The goal of data management is to improve organizational efficiency.

Data management is solely and exclusively related to the business data generated during the work.

Knowledge is essential for the effective operation of the organization and for the continuous improvement of efficiency

- suitability and effectiveness of existing business processes,
- adequacy and utilization of business applications,
- the workload and the appropriate preparedness of the existing human resources
- adequacy and effectiveness of existing regulations.

In order to improve organizational efficiency, availability of ad-hoc information is not sufficient, but the entire service cycle and the support organization as a whole must be captured in accordance with the service levels undertaken. This is defined by senior management through the definition of specific Business Indicators (KPIs), and the IT elements of the JC360 service are customized accordingly to determine the scope of data collected in a given position.

Data collection is therefore carried out solely for the purpose of the legitimate interest of assessing and improving organizational effectiveness while doing work.

The legal basis for data management is Article 6 (1) (f) of the GDPR, the legitimate interest of the employer.

Disclosure of responsibilities related to data management

Name of Data Manager: [Name of organization using JC360]

Information of the Data Processor: JobCTRL Informatikai Kft.; 1118 Budapest, Rétköz st. 7.; registration number: Cg. 01-09-949636; represented by: Ferenc Perjés director; telephone: +36 1 465 8808; e-mail: support@jobctrl.com

In particular, the Data Manager shall be responsible for:

- determining which positions are covered by the JC360 service measurement,
- definition of data management conditions: what purpose should be introduced for the JC 360 service, what data scope should be covered by the processing of the JC360 service, how long this data is stored,
- conducting a legitimate interest opinion of the legal basis for data management,
- determining who within the data manager's organization system will have access to the processing result of the JC360 service,
- advance notice to employees of the JC360 service,
- entering into a data processing contract with JobCTRL Kft.,
- conducting a privacy impact assessment.

In particular, the Data Processor shall be responsible for:

- executing data manager instructions: If the data manager (team leader, admin authority) deletes data, changes settings, authorizes in connection with the JC360 service then the software shall actually perform these actions
- secure storage of data on the JC360 server resulting from the processing of the JC360 service (meeting the data security requirements of Article 32 of the GDPR),
- if additional data processor is used (such as subcontracting to provide the service) in connection with the JC360 Service, they shall be responsible for the operations of that data processor.

Does the Data Processor have any certification?

JobCTRL Kft,, as data processor has ISO27001 ceertification..

Data, the data management process, data management tools

The scope of personal data processed

Pursuant to Article 4 (1) of the GDPR, data relating to the work activities of the Employee may also be considered as personal data.

Data collection related to JC360 service IT support is performed only in an on and off state.

Data collection related to JC360 service IT support can be controlled (enabled / disabled) at an organizational / group / employee level. The following list describes the full set of options that may be different (less) from the custom organizational setting.

The JC360 PC Client can record the following data in working (green) state:

- Job task selected in JC360 ("Job" by default, but this can be expanded and changed with rules, eg change to "SAP use" task in SAP.exe)
- The name of the active application (eg explorer.exe) and address bar
- The value of the URL field in the active window of supported browsers (Internet Explorer, Chrome, Mozilla Firefox)
- In the supported mail client (Outlook, corporate Gmail, Lotus Notes), the From, Email, Subject, fields
- For supported office applications (Microsoft Office, Acrobat Reader), name and path of the opened document
- Computer Usage Intensity Indicator (number of mouse and key activity per minute based on real activity)
- 30 second sampling of on-screen app images (blurry levels: good / medium / bad / censored) - off by default
- Individual processing points (eg contract ID, customer ID) if required by the data manager

The JC360 Mobile Client can record the following data in working (green) state:

- Job task selected in the JC360 mobile application ("Job" by default, but this can be expanded and changed with rules, eg change to "Mail" task in email application)
- GPS positions
- Non-private phone numbers (caller / called) and call duration
- Name of active applications
- Photos taken manually with the mobile device from the JC360 mobile app with attached notes.
- Note that can be freely edited or selected from a predefined hierarchical structure,
- Individual processing points if required by the data manager (eg POI name is stored for GPS based POI determination)

Collected data is stored by default in the system for 5 years, but can be individually configured at the organizational / group / employee level (in days). The storage period is calculated from the moment of collection, after that, the data is permanently deleted.

Deletion of the collected data can be viewed and permanently deleted from the system by the employee at any time within the set time (1 week by default). Administrators can permanently delete arbitrary periods of any employee at any time.

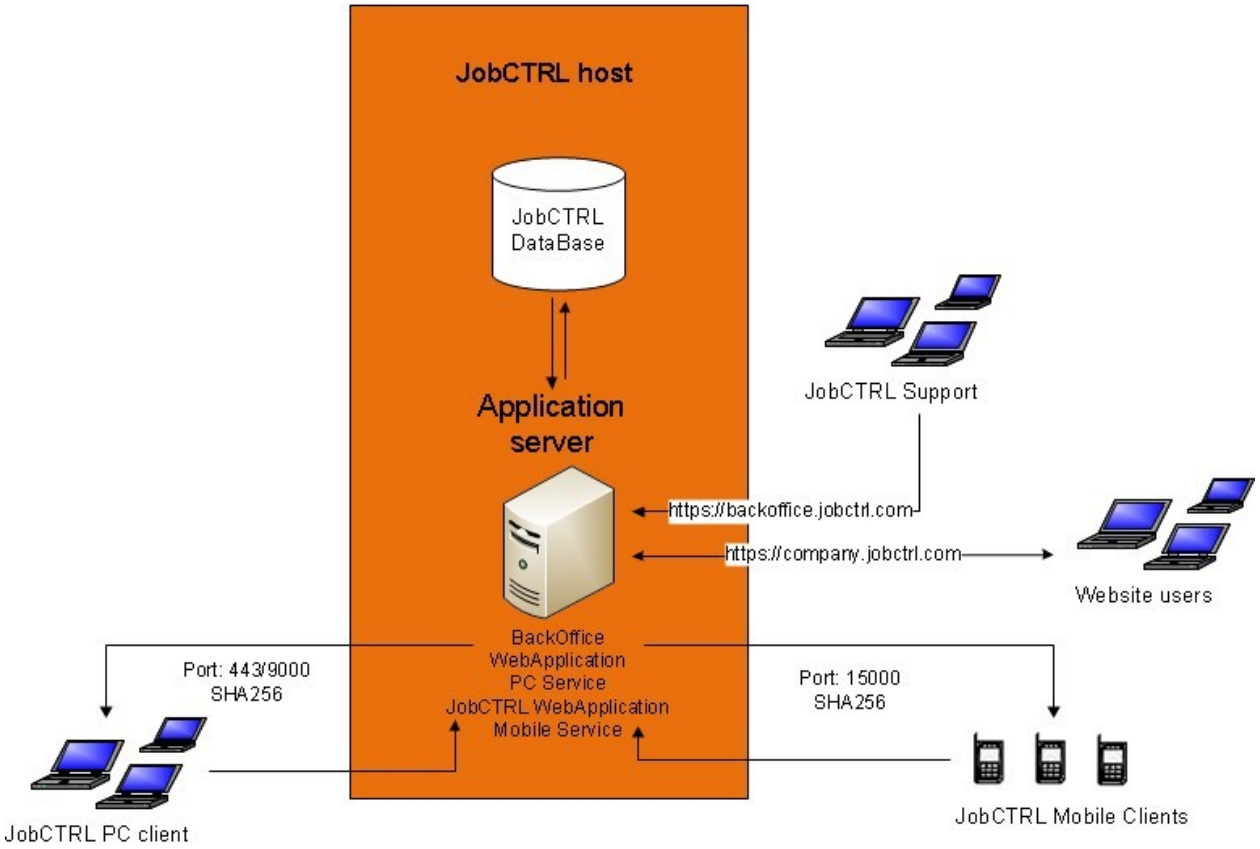
The collected data is stored in a closed system. Access to the data can be controlled by the Data Manager / Employee / Team Leader / Admin authority and can only be accessed through authorized target reports.

Admin controls the admission of target reports, which can be waived by other Admin users. Target reports can be enabled / disabled at the organization / group / employee level.

The employees can see all data about themselves in the authorized target reports. The team leaders can see the details of themselves and their assigned employees in their authorized target reports. Admin can see everyone's data in their authorized target reports

Presentation of the data management processes

For the data flow architecture see:



The entry point for data management is as follows:

- the employees concerned must be registered and activated in the JC360 system (notified by letter)
- the employees concerned create themselves a password (which must comply with safety regulations)
- the JC360 client application must be installed on the work equipment concerned (this can be done by the employee according to the instructions in the letter or centrally managed by IT).
- the client program must be started and logged on. It is possible to select "Remember" so that the client will not request a login when restarting the machine. This check box is not enabled by default.

The IT solutions that support the JC360 service provide the user with the purpose of the Data Management and provide a direct link to the detailed Privacy Statement (which can be viewed at any time in the future) ont he first run in a window. This window will disappear when you click on the OK button. The time of clicking the OK button will be saved and will be considered as the date of acknowledgment of the information.

The client can be out of work and in a working state and informs the user by color indication (red / green) and writing (bubble). In the working (green) state, data is collected according to the configuration for the current user. The collected data is encrypted and sent to the local computer and periodically transferred to the JC360 server using SSL encryption when the network is active. In this case, the data is deleted from the local computer.

At any time, the user can view the collected data in the client application and modify or delete them. They can also log in to the JC360 and view the available information and change the settings.

The user has the ability to create their own rules, such as a temporary logout rule, which automatically sets the client to a non-working (red) status for any application / URL, stopping data collection.

The collected data can be viewed by users through the specified target reports and can be modified and deleted within a pre-set time (1 week by default).

The data is stored on the JC360 server and automatically deleted from it (within 5 years by default). Admin can permanently delete data for any period of time and for any user.

The data can only be accessed through the target reports specified by the data manager, at the level of aggregation specified therein, according to the appropriate authorization settings (worker / team leader).

Data will be managed in accordance with internal policies of the data manager throughout the data management process.

What are the tools for managing personal data?

The scope of data collected during the JC360 service and the recommended target reports are the result of the extensive configurability described above.

The JC360 PC Client can be used in Windows, Macintosh and Linux environments.

The JC360 mobile Client can be used in Android and IOS environments.

The JC360 server uses the Windows operating system and Microsoft SQL database. The servers may be hosted by the organization in its own environment, in the ISO27001-certified TIER4 data room of the JobCTRL Kft., or one of the JC360 servers of Microsoft Azure.

JC360 target reports can be received in a downloaded form (XLS), emailed (HTML email), targeted message ("bubble"). The definition of target reports also covers the form of creation.

BASIC PRINCIPLES

Proportionality and necessity

Are the purposes of data management defined, clear and legitimate?

The goal of data management is to improve organizational efficiency.

Data management is solely and exclusively related to the business data generated during the performance of work. (definition)

Knowledge is essential for the effective operation of the organization and for the continuous improvement of efficiency (clarity)

- suitability and effectiveness of existing business processes,
- adequacy and utilization of business applications,
- the workload and the appropriate preparedness of the existing human resources
- adequacy and effectiveness of existing regulations.

In order to improve organizational efficiency, availability of ad-hoc information is not sufficient, but the entire service cycle and the support organization as a whole must be captured in accordance with the service levels undertaken. This is defined by senior management through the definition of specific Business Indicators (KPIs), and the IT elements of the JC360 service are customized accordingly to determine the scope of data collected in a given position.

Data is collected solely for the purpose of carrying out the work and for the legitimate interest of assessing and improving organizational effectiveness. (legitimacy).

What is the legal basis for data management?

The legal basis for data management is Article 6 (1) (f) of the GDPR, the legitimate interest of the employer.

Are the data collected appropriate and relevant for the purposes of data management and limited to what is necessary (data saving)?

The scope of data collected will be derived for data management purposes during the implementation of the JC360 service. Data Manager, as represented by the data processor, determine the business metrics (KPIs) included in the target reports, and only the data necessary for this purpose are collected and displayed.

Is the data accurate and up-to-date?

The collected data is collected into a closed system, directly from the data source (active application). However, the user has the option to view and modify or delete the data within the time limit (1 week by default). The essential part of the data is the data related to the given job, so keeping it up-to-date is not relevant, and it is expressly forbidden to modify it later.

What is the period of data retention?

The data can be set at the organizational / group / employee level by Admin. By default, the retention period is 5 years.

Measures to ensure the rights of data subjects

How are the subjects informed about data management?

The IT solutions that support the JC360 service provide the user with the purpose of the Data Management and provide a direct link to the detailed Privacy Statement (which can be viewed at any time in the future) ont he first run in a window. This window will disappear when you click on the OK button. The time of clicking the OK button will be saved and will be considered as the date of acknowledgment of the information. Of course, this can be preceded by other organizational information, so typically the subjects will be informed in accordance with the internal processes and regulations of the Data Manager. In addition, the immediate manager may inform their immediate subordinates in writing and verbally.

If data management is based on consent, how are the consent of the subjects obtained?

Not relevant.

The legal basis for data management is Article 6 (1) (f) of the GDPR, the legitimate interest of the employer.

How can data subjects enforce their right of access and data portability?

Subjects have direct access to the data stored about them at any time through dedicated reports.

Upon request, admin authorized users of the data manager have the right to download all stored data in a dedicated workflow report ("workflow report"), which allows for data portability.

How can stakeholders exercise their right to rectification and erasure?

Subjects have direct access to the data stored about them at any time through dedicated reports. Data can be modified or deleted at any time within the time window that applies to them.

Modification of data is not possible for business data related to system lock (eg document name, duration), such data can only be erased. Modifications can only be made to data specified by the employee, eg. the name of the Job Task.

In addition to the time window, the Admin user of Data Manager can permanently delete any time period and employee and any data set.

How can data subjects exercise their right to restrict data processing and right to object?

Subjects can at any time directly access data management restrictions by turning off the non-working status (red), exiting the program, or using built-in modification capabilities of the JC360-enabled IT solution client program.

Pursuant to Article 18 (1) of the GDPR, the right to restrict data processing to the JC360 service is as follows:

- if the personal data collected by the JC360 service is inaccurate and up-to-date according to the data subject, the data manager must suspend data processing for the period during which it verifies the accuracy of the data;
- if data processing is unlawful (for example, NAIH has determined this) and the data subject objects to the deletion of personal data, the data subject is entitled to request that the data collected by the JC360 Service be restricted (locked),
- if the data manager no longer needs the data collected by the JC360 service, but the data subject requires it for the purpose of submitting, asserting or defending legal claims,
- if the data subject objects to the data manager (employer) employing the JC360 in connection with them, then the data manager must suspend the data collection for this employee for a period of time to investigate whether the arguments raised by the employee override the legitimate interests of the manager.

Subjects may initiate restrictions on data management at the organizational level primarily through the designated data processor of the data manager or by the immediate superior, who will then conduct the procedure in accordance with the internal regulations of the organization.

Are the obligations of data processors clearly stated in the data processing contract?

Information of the Data Processor: JobCTRL Informatikai Kft.; 1118 Budapest, Rétköz st. 7.; registration number: Cg. 01-09-949636; represented by: Ferenc Perjés director; telephone: +36 1 465 8808; e-mail: support@jobctrl.com

The data processing contract is based on the provisions of Article 28 of the GDPR and in accordance with the provisions of the applicable national law, modified by the Data Protection Lawyers as necessary in accordance with the internal regulations and signed by the parties. In the absence of a signature, the authorized representative of the Data Manager has accepted the Terms and Conditions in a documented manner.

Is personal data adequately protected when transmitting data outside the European Union?

Not relevant.

The data is stored on servers in the given country, so in the case of EU citizens, within the EU. The Data Manager can also decide to store data internally at any time by setting up an internal server.

RISKS

Planned or existing measures

Encryption

The stored data is encrypted on the client devices and transmitted to the server via an encrypted channel (HTTPS). In the database, users' passwords are stored with one-way encryption.

Encryption algorithm

SHA-256 RSA encryption,

Data is transmitted with 2 key encryptions

Segregation of data

The information is personalized based on the employee's name and email address. This data is stored in a separate data table and assigned a unique identifier.

Each data is located in a separate data table and the cross references are made with identifiers. Thus, for them, understanding the data structure is time consuming and concise.

Therefore, data of the job are stored only with an identifier, so a possible incident makes it significantly more difficult to personalize the data.

Logical access control

The collected data is stored in a closed system. Access to the data can be controlled by the Data Manager / Employee / Team Leader / Admin authority and can only be accessed through authorized target reports.

Admin controls the admission of target reports, which can be waived by other Admin users. Target reports can be enabled / disabled at the organization / group / employee level.

The employees can see all data about themselves in the authorized target reports. The team leaders can see the details of themselves and their assigned employees in their authorized target reports. Admin can see everyone's data in their authorized target reports.

Traceability (logging)

Major sensitive data events of the IT solutions supporting the JC360 service are logged. This allows you to determine who, when and what you changed (from-> to). This is especially true for data impersonating data and changing the scope of data collected.

Each activity can be tracked in the system with a time stamp. Log entries are stored in a database so they can be easily linked to other logging systems and log evaluators.

Data minimization

the scope of data collected will be derived for data management purposes during the implementation of the JC360 service. Data Controllers, as represented by the Data Manager, determine the business metrics (KPIs) included in the target reports, and only the data necessary for this purpose are collected and displayed.

The information is personalized based on the employee's name and email address. This data is stored in a separate data table and assigned a unique identifier. Data regarding employees is stored only with an identifier, so any incident can make it very difficult to personalize the data.

Website Security

The JC360 service website is available with HTTPS encryption.

OWASP standards are developed.

Regular penetration tests are performed on the system according to the QUALYS PCI DSS penetration testing.

The relevant procedures are carried out in accordance with ISO27001 standards and regulations.

Backup

Backups may be made in accordance with the own internal policies of the data manager.

Network Security

Data is transmitted on the network exclusively in encrypted form. (SSL certified)

Handling of personal data breaches

The data processor shall notify the data manager within 24 hours, taking into account article 33 of the gdpr, of personal data incidents.

Regulations

The data manager must apply its own permissions policies for accessing the IT components of the JC360 service.

Unauthorized access to data

What would be the main consequences for those affected if the risk were to occur?

Work Time, Work Apps, URLs, Work Correspondence (Sender, Recipient, Subject), Mobile Work Call (Caller / Caller, Duration), Work Use Documents, Mobile GPS Work Stay, Work knowledge of data, violation of the goodwill of the Employee and respect in the workplace

What are the main emerging threats that may pose the risk?

Improper handling of permissions, Unauthorized use of existing permissions

What are the sources of risk?

Admin users, Invalid authorization management

Which of the available measures serve to manage the risk?

Data Segregation, Traceability (Logging), Data Minimization, Website Security, Policies, Logical Access Control, Dealing with Personal Data Violations

How is the severity of the risk assessed, in particular with regard to its possible consequences and the risk management measures envisaged?

Insignificant, basically this is only data collected during work. Unauthorized access to these data does not pose any particular risk to the data subject, as their content is essentially information that can be accessed by other employees of the company.

Severity may be classified into two categories:

- On the one hand, the severity of the effect is Insignificant when the data collected by the JC360 service indicates that the employee is performing at a similar or higher standard (results) to other employees. In this case, unauthorized access to personal data can be a simple annoyance, a feeling of interference in the privacy of the employee, without any real or objective harm.
- On the other hand, the severity of the effect is Insignificant or limited if the employee's measurement data deviates significantly from the performance of other employees in similar jobs. Severity obviously also depends on the employee's sensitivity, as it can be a source of annoyance for them, but they may feel unauthorized access to their reputation or reputation for work, and this should be seen as a limited consequence. However, in the latter case too, the sense of privacy violation does not mean irreversible, significant harm to the employee.

In addition, two other circumstances need to be highlighted. On the one hand, the data collected by the JC360 service is stored encrypted and transmitted over an encrypted channel, so that if they are accessed unauthorized, they cannot be decrypted into personal data. On the other hand, reducing the severity of the risk is the fact that employee data is stored solely with an ID so that in the event of a malicious attack outside the organization, the person acquiring personal data cannot link the data to an identified individual.

In view of this, our "conclusion" is that the severity of the consequences of unauthorized access is fundamentally Insignificant.

How do you assess the likelihood of a risk, in particular in view of emerging threats, sources of risk and planned risk management measures?

Insignificant, Access levels are established with the help of JC360 Consultants when the JC360 service is deployed. Thereafter, the data manager shall be maintained in accordance with its internal regulations.

Given the security measure described earlier in the privacy impact assessment, the likelihood of this is Insignificant (for example, by virtue of internal policies, access workers are aware of the consequences of unauthorized access to personal data).

Accidental or unauthorized alteration of data

What would be the main consequences for those affected if the risk were to occur?

False data on individual performance, false data on organizational performance, unjustified management interference, breach of employee reputation, workplace reputation

What are the main emerging threats that may pose the risk?

Conscious database level attack, Unauthorized access

What are the sources of risk?

Admin users, Invalid authorization management

Which of the available measures serve to manage the risk?

Rules, Data Segregation, Traceability (Logging), Logical Access Control

How is the severity of the risk assessed, in particular with regard to its possible consequences and the risk management measures envisaged?

Limited,

Severity may be classified into two categories:

- On the one hand, the severity of the consequences if personal data collected by the JC360 service is accidentally or unlawfully modified to improve the employee's performance is Insignificant. This has no serious consequences for the employee.
- On the other hand, the severity of the consequence if the employee's measurement data via the JC360 service is significantly changed is Insignificant or limited. Severity obviously also depends on the employee's sensitivity, as this can mean simple annoyance, but it may be that he or she feels that his or her reputation, his or her reputation for work, has been damaged by accidental or unlawful alterations. However, in the latter case too, the feeling of privacy violation does not mean irreversible, significant harm to the employee.

Any malicious modification of the data could result in undue management interference. However, for executives, the JC360 primarily produces only decision-making data, which is followed by stakeholder consultation before making its own decisions, so that the severity of an ad hoc point-by-point malpractice modification could have a limited impact.

How is the severity of the risk assessed, in particular with regard to its possible consequences and the risk management measures envisaged?

Insignificant, Organizational and individual performance is made up of complex, complex relationships, so an occasional, point-by-point malicious data modification practically prevents the occurrence and real impact of this risk.

The measures taken further reduce the likelihood of the risk occurring.

Given the security measure described earlier in the data protection impact assessment, the likelihood of this is Insignificant (for example, employees with access due to internal regulations are aware of the consequences of unauthorized modifications to personal data).

Data Loss

What would be the main consequences for those affected if the risk were to occur?

Absence of analytics on organizational and invidual performance, Data relating to period of data loss

What are the main emerging threats that may pose the risk?

Unjustified Admin deletion, Time window too broad

What are the sources of risk?

Inappropriate handling of rights, Improper configuration

Which of the available measures serve to manage the risk?

Backup saving, Tracking option (logging), Policies, Website safety

How is the severity of the risk assessed, in particular with regard to its possible consequences and the risk management measures envisaged?

Insignificant, Partial data loss does not significantly affect statistical-based estimates. However, data can be restored from backups if needed.

A special feature of the JC360 service is that it has no negative consequences for the privacy of employees, and there is no risk of data loss, as if the data measured by the JC360 service is lost, neither their privacy nor their employment will be affected. Accordingly, from the employees' point of view, even a Insignificant risk of data loss cannot be identified.

How is the severity of the risk assessed, in particular with regard to its possible consequences and the risk management measures envisaged?

Insignificant, Configuration is checked by JC360 service consultants, so the timelines available for deletion are thus controlled for appropriateness. Admin users receive training on how to use the features, so the risk of accidental data deletion is low.

ACTION PLAN

Basic Principles

No notified action plan.

Existing or planned measures

No notified action plan.

Risks

No notified action plan.

Illegitimate access to data

Severity : Negligible

Likelihood : Negligible

Unwanted modification of data

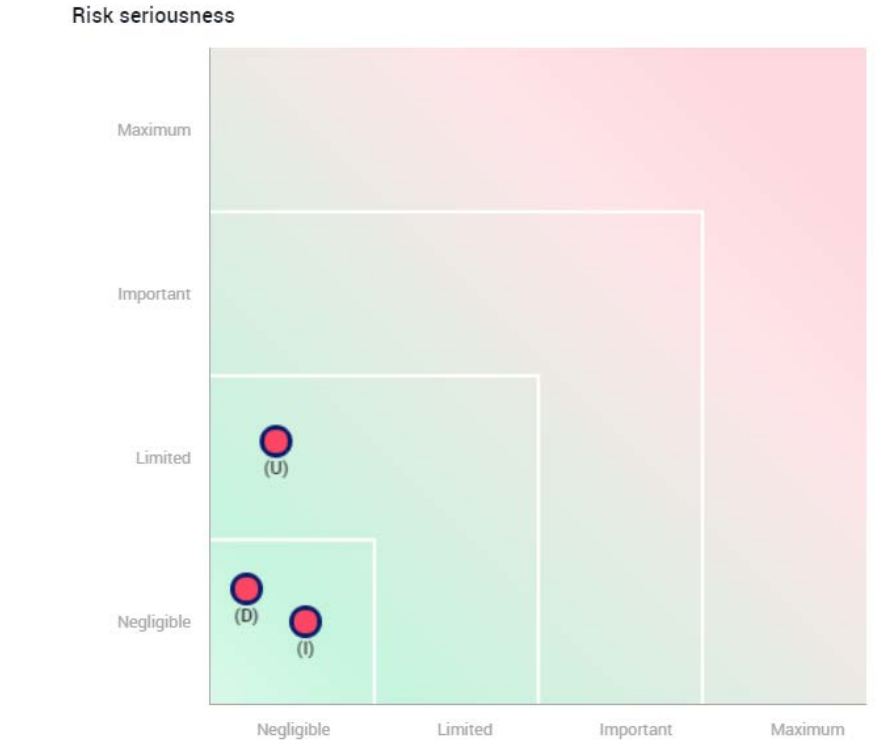
Severity : Limited

Likelihood : Negligible

Data disappearance

Severity : Negligible

Likelihood : Negligible



- Planned or existing measures
- With the corrective measures implemented
- (I)llegitimate access to data
- (U)nwanted modification of data
- (D)ata disappearance

LEGITIMATE INTEREST'S ASSESSMENT

Table of contents

This legitimate interest's assessment (LIA) template is suggested by ICO, the UK's independent authority set up to uphold information rights in the public interest, promoting openness by public bodies and data privacy for individuals. It is available at https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/legitimate-interests/how-do-we-apply-legitimate-interests-in-practice/

PART 1: PURPOSE TEST

You need to assess whether there is a legitimate interest behind the processing.

1. Why do you want to process the data?
2. What benefit do you expect to get from the processing?
3. Do any third parties benefit from the processing?
4. Are there any wider public benefits to the processing?
5. How important are the benefits that you have identified?
6. What would the impact be if you couldn't go ahead with the processing?
7. Are you complying with any specific data protection rules that apply to your processing (eg profiling requirements, or e-privacy legislation)?
8. Are you complying with other relevant laws?
9. Are you complying with industry guidelines or codes of practice?
10. Are there any other ethical issues with the processing?

1. Why do you want to process the data?

The goal of data management is to improve organizational efficiency.

2. What benefit do you expect to get from the processing?

Knowledge is essential for the effective operation of the organization and for the continuous improvement of efficiency

– suitability and effectiveness of existing business processes,
– adequacy and utilization of business applications,
– the workload and the appropriate preparedness of the existing human resources
– adequacy and effectiveness of existing regulations.

In order to improve organizational efficiency, availability of ad-hoc information is not sufficient, but the entire service cycle and the support organization as a whole must be captured in accordance with the service levels undertaken. This is defined by senior management through the definition of specific Business Indicators (KPIs), and the IT elements of the JC360 service are customized accordingly to determine the scope of data collected in a given position.

3. Do any third parties benefit from the processing?

Analyzing and improving the efficiency of an organization is in the interest of all employees, subcontractors, business partners and clients within the organization. This allows employees and subcontractors to receive competitive wages / fees and customers to receive quality service.

Ineffective operation leads to the organization becoming unprofitable, which makes operation impossible and leads to the dissolution of the organization.

4. Are there any wider public benefits to the processing?

Analyzing organizational efficiency enables focused and efficient organizational development and an objective evaluation of corporate value creation. Transparency also allows for the wider use of flexible forms of employment and tele-working within the organization.

On this basis, the services of the organization will be optimized and cost-effective for the general public, and will contribute to the achievement of social objectives by promoting flexible employment.

5. How important are the benefits that you have identified?

The benefits identified above are a natural part of the organization's operations. Analyzing organizational effectiveness through the JC360 becomes an active component of process design, training materials, objective performance evaluation, and optimal service levels.

6. What would the impact be if you couldn't go ahead with the processing?

Without JC360-based development, current efficiency and effectiveness are expected to stagnate, and failure to provide this development opportunity is an unacceptable loss in the current market environment. In addition, there is no other way to ensure an equal sharing of workload between employees.

7. Are you complying with any specific data protection rules that apply to your processing (eg profiling requirements, or e-privacy legislation)?

At JC360, we comply with applicable legal and professional regulations and meet the requirements regarding our service. Accordingly, we have taken into account and comply with

– the requirements of Regulation (EU) 2016/679 of the European Parliament and of the Council (General Data Protection Regulation, GDPR Regulation) 1, according to which the data collected and analyzed are personal data,

[1] https://eur-lex.europa.eu/legal-content/HU/TXT/?uri=CELEX:32016R0679

– the WP251.rev.01 Data Protection Working Party Guideline on Profiling2, as the use of the JC360 service implies that the Data Controller may profile the employees based on the data collected (in which case the Controller may have additional responsibilities),
– the November 2016 Brief of the Hungarian National Authority for Data Protection and Freedom3 on Information Key Requirements for Workplace Data Management, which set out requirements in the context of its legal basis for legitimate interest opinion,
– the Hungarian National Authority for Data Protection and Freedom of Information Recommendation on Prior Information Requirement of October 2015 4, which sets out the expectations of the authority regarding data processing information,
– ISO / IEC 27001: 2013 Information Security Standard5, which is overseen by the International Organization for Standardization (ISO) and the International Electrotechnical Commission6 (IEC) and is certified by the Hungarian Standards Board and IQcert7.

8. Are you complying with other relevant laws?

The applicable data management and data processing complies with all applicable legal requirements.

In this respect, it is worth highlighting (EU) 2016/679 Regulation of the European Parliament and the Council (General Data Protection Regulation, GDPR Regulation) [8] and Act I of 2012 of the Hungarian Labor Code (hereinafter: Labor Code) as provisions of which are compliant with the data management of the JC360 service. Article 9 (2) of the Labor Code requires that "an employee's right to privacy may be restricted if, for reasons directly related to the purpose of the employment relationship, the restriction is strictly necessary and proportionate to the achievement of the purpose." Conducting a legitimate interest opinion and conducting a privacy impact assessment provide assurance that the JC360 service is necessary and proportionate to the achievement of the purpose of protecting employees' personal data. Conducting a test of interest and conducting a privacy impact assessment provide assurance that the JC360 service is necessary and proportionate to the achievement of the purpose of protecting employees' personal data. In addition, Article 9 (2) of the Labor Code requires that "the employee must be informed in writing in advance of the manner, conditions and probable duration of the limitation of the right to an individual right, as well as the circumstances justifying its necessity and proportionality." The

[2] https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612053
[3] http://naih.hu/files/2016_11_15_Tajekoztato_munkahelyi_adatkezelesek.pdf
[4] http://naih.hu/files/tajekoztato-ajanlas-v-2015-10-09.pdf
[5] https://en.wikipedia.org/wiki/ISO/IEC_27001
[6] http://prod.mszt.hu/hu-hu/tanusitas/tanusitasi-szolgaltatasok/informaciobiztonsag-iranyitasi-rendszerenek-tanusitasa
[7] http://www.iqcert.co.uk/
[8] https://eur-lex.europa.eu/legal-content/HU/TXT/?uri=CELEX:32016R0679

employer, as data controller, has prior notice of the JC360 service and thus complies with this requirement of the Labor Code.

9. Are you complying with industry guidelines or codes of practice?

In the course of data management, we follow the relevant regulations and recommendations and constantly monitor for changes (Hungarian National Authority for Data Protection and Freedom of Information, ICO, GDPR). In addition, we are members of professional organizations (eg ISACA, IVSZ), have certifications (eg ISO27001, CISO, CISA) and fully comply with development standards (eg OWASP).
10. Are there any other ethical issues with the processing?
Given that data management only applies to work-related activities, there is no known ethical problem.

PART 2: NECESSITY TEST

You need to assess whether the processing is necessary for the purpose you have identified.

1. Will this processing actually help you achieve your purpose?
2. Is the processing proportionate to that purpose?
3. Can you achieve the same purpose without the processing?
4. Can you achieve the same purpose by processing less data, or by processing the data in another more obvious or less intrusive way?

1. Will this processing actually help you achieve your purpose?

The JC360 Service Pack enables you to analyze and improve organizational efficiency with innovative, in-process business metrics. This makes the goals described in the previous paragraph much faster, more accurate, cheaper and more comprehensive than our existing processing systems. The JC360 provides 100% online sampling, but with approaches based on sampling and estimation to date.
We aim to increase efficiency and effectiveness by measuring and analyzing work efficiency KPIs in selected positions. The fluctuation, scatter and trend analysis of the value of each business indicator gives us an accurate picture of the opportunities for development within the company, the needs for change, and helps us to achieve an even work distribution.

2. Is the processing proportionate to that purpose?

Data management is solely and exclusively related to the business data generated during the work.

Data collection is therefore carried out only and exclusively for the purpose of carrying out the work, in the interest of assessing and improving organizational effectiveness.

3. Can you achieve the same purpose without the processing?

No. Without the JC360 service, it is not possible to get up-to-date, comprehensive analysis of organizational efficiency and achieve such efficient organizational development.

4. Can you achieve the same purpose by processing less data, or by processing the data in another more obvious or less intrusive way?

Data management is basically limited to a restricted set of data, certain personal data generated during work, and the JC360 service does not monitor all work. Therefore, data management shall not be considered "intrusive" to the privacy of the employee.

Another important feature of the software is that the employee can turn the service on and off and always have access to their own personal information, so it is completely clear for them how data management works.
In addition, the scope of data collected will be derived for data management purposes during the implementation of the JC360 service. Data Controllers, as represented by the Data Manager, determine the business metrics (KPIs) included in the target reports, and only the data necessary for this purpose are collected and displayed.

PART 3: BALANCING TEST

You need to consider the impact on individuals' interests and rights and freedoms and assess whether this overrides your legitimate interests.

First, use the DPIA screening checklist. If you hit any of the triggers on that checklist you need to conduct a DPIA instead to assess risks in more detail.

Nature of the personal data

1. Is it special category data or criminal offence data?
2. Is it data which people are likely to consider particularly 'private'?
3. Are you processing children's data or data relating to other vulnerable people?
4. Is the data about people in their personal or professional capacity?

1. Is it special category data or criminal offence data?

No. Data management is only and exclusively related to the business data generated during the work. Accordingly, data is data stored on devices and IT applications owned by the organization's business.

2. Is it data which people are likely to consider particularly 'private'?

No. Data management is done specifically on the basis of business data generated during the work. For private activities, the user can turn off the processing, set an automatic exit rule (eg for Internet banking), and recorded data can be deleted retrospectively (in a default time window, by default for 1 week).

3. Are you processing children's data or data relating to other vulnerable people?

No. No sensitive data regarding children, health or other will be stored.

4. Is the data about people in their personal or professional capacity?

Yes, the data collected is suitable for comparative analysis of individual performance (relative to group average, organizational expectations). For this reason, we also conducted a Privacy Impact Assessment on the use of the JC360 service.

Reasonable expectations

1. Do you have an existing relationship with the individual?
2. What's the nature of the relationship and how have you used data in the past?
3. Did you collect the data directly from the individual? What did you tell them at the time?
4. If you obtained the data from a third party, what did they tell the individuals about reuse by third parties for other purposes and does this cover you?
5. How long ago did you collect the data? Are there any changes in technology or context since then that would affect expectations?
6. Is your intended purpose and method widely understood?
7. Are you intending to do anything new or innovative?
8. Do you have any evidence about expectations – eg from market research, focus groups or other forms of consultation?
9. Are there any other factors in the particular circumstances that mean they would or would not expect the processing?

1. Do you have an existing relationship with the individual?

Yes, data management is done on the business data generated by the work of those who work in association with the organization. Thus, the affected parties are employees, subcontractors.

2. What's the nature of the relationship and how have you used data in the past?

The relationship is basically based on an employment relationship.
The "legal background" to the processing of JC360 is provided by Article 42 (2) (a) of the Labor Code, which states that "under the employment contract, the employee is required to carry out work under the direction of the employer". On the other hand, Article 52 (1) (b) to (d) of the Labor Code provides the background for data management. Pursuant to these provisions of the Labor Code, the employee must be available to the employer for work during working hours, to carry out their

work personally, with the generally expected skill and care, to comply with the rules, regulations, instructions and habits of their work and to exhibit trustworthy behavior in order to perform their work. Those provisions essentially mean that the worker is obliged to work during their working hours and that the employer may legitimately assume that the worker is working during his working hours. The employer has a large degree of freedom in organizing work or the performance of duties related to the job, within the limits set by the Labor Code. Depending on the business and economic interests of the employer, they may determine, by task and by work process, how the employee is to perform his job. In order to exercise this power of direction, the employer must have a clear picture of how the employees are performing their duties.
Work data has always been collected and analyzed by the organization (eg application logs, lead times), but so far it has been case-based, based on sampling or estimation and has therefore produced less accurate results than the JC360 service.

3. Did you collect the data directly from the individual? What did you tell them at the time?

Data management starts and stops directly under the influence of the employee, and the data are generated only in the course of their activity.

The IT solutions that support the JC360 service provide the user with the purpose of the Data Management and provide a direct link to the detailed Privacy Statement (which can be viewed at any time in the future) ont he first run in a window. This window will disappear when you click on the OK button. The time of clicking the OK button will be saved and will be considered as the date of acknowledgment of the information.

Of course, this can be preceded by other organizational information, so typically the subjects will be informed in accordance with the internal processes and regulations of the Data Controller. In addition, the immediate manager may inform their immediate subordinates in writing and verbally.

4. If you obtained the data from a third party, what did they tell the individuals about reuse by third parties for other purposes and does this cover you?

Not relevant, data is not obtained from a third party.

5. How long ago did you collect the data? Are there any changes in technology or context since then that would affect expectations?

This is a new type of data management, personal data was not collected previously by using this method, for this purpose, and the result of the technological and IT developments is the ability to analyze data using such software.

Since the launch of the JC360, there has been no change that calls into question the purpose and necessity of data management.

6. Is your intended purpose and method widely understood?

The purpose and principle of data management are clear to all concerned. The briefings and regular weekly target reports give them an accurate picture of the value and trends of the data collected and of them and the team.

7. Are you intending to do anything new or innovative?

The result of the data management is used in the business targets (KPIs) and target reports. Analyzing and improving organizational effectiveness may require the creation of new indicators, and data collection will be adjusted accordingly. This allows for a "continous improvement" approach, so innovation can be reached practically every few months.

8. Do you have any evidence about expectations – eg from market research, focus groups or other forms of consultation?

Measuring organizational efficiency is a typical activity in the industry, both for employees and for employees. Only the tools and methods change. Measuring, analyzing and improving efficiency is a logical step to meet changing market demands, staying ahead of competitors, and achieving cost-effective operation.

The Organization has informally consulted employees prior to commencing data processing and is aware that the expectations of employees regarding the use of software that analyzes their work performance. These expectations include, for example: the ability to turn off the processing of the JC360, allowing them to see, adjust, and, if necessary, access the processing data only to a very limited extent within the employer's organizational system, etc.

9. Are there any other factors in the particular circumstances that mean they would or would not expect the processing?

There is no such circumstance as employees receive information from the employer about the JC360 processing and data management, and they can turn the processing on and off themselves, so they are fully aware of the data management.

Likely impact

1. What are the possible impacts of the processing on people?
2. Will individuals lose any control over the use of their personal data?
3. What is the likelihood and severity of any potential impact?
4. Are some people likely to object to the processing or find it intrusive?
5. Would you be happy to explain the processing to individuals?
6. Can you adopt any safeguards to minimise the impact?

1. What are the possible impacts of the processing on people?

Data management is done through the business data generated by the work of those who work in association with the organization.

The only negative impact on individuals may be the possible violation of privacy protection (eg private activity is recorded).

2. Will individuals lose any control over the use of their personal data?

Recording private activities expressly not a purpose of data management. As a result, multiple devices are available to users, as follows:

1. Potentially private pages are centrally controlled, in which case the data collection of the JC360 client software is suspended (eg social networks, magazines, internet banks)
2. The user can turn off (red) data collection at any time
3. User can create their own rules, which automatically disables data collection (eg defining a private browser, logging off to their own web pages)
4. In case the data be collected, the user has the option to permanently delete their data within a time window (1 week by default)
5. If you exceed the time window, you can request the deletion of your data from your immediate supervisor at any time for a specific period.

These controls are described in detail in the Privacy Impact Assessment document.

3. What is the likelihood and severity of any potential impact?

Due to the controls and automations described in the previous paragraph, the likelihood of a risk is very low.
The severity of the risk is reduced primarily by the fact that if a private activity were recorded, it would not be named in analytics. Target reports essentially display business metrics (KPIs), which do not include aggregate data (such as transaction time) and elementary details (such as a URL).

4. Are some people likely to object to the processing or find it intrusive?

Given the purpose of data management, less-performing employees are expected to attack this objective, transparent solution. However, for the majority, the JC360 is a really useful option, that can make us an organization of the 21th century, creating a culture of real and fact-based value-centered organization through flexible employment.

Activities of Employees are subject to many regulations in the workplace. There are rules for using the computer, using office tools, and using applications. Thus, the JC360 service currently analyzed during work is not expected to be particularly distracting to those affected.

5. Would you be happy to explain the processing to individuals?

Of course it is, because the basic element of the system itself is that the employee switches the processing on and off, and is visibly notified.
Measuring, analyzing and improving organizational efficiency is an inevitable element for market players in our industry. We have done processing so far and our evaluation system was based on them. This measurement only makes our measurements and analyzes more complete, accurate and up-to-date, so we can design, develop and process them in a more focused and efficient manner. This is something that all our employees need to understand, because the success of an organization is also the foundation of their work.

6. Can you adopt any safeguards to minimise the impact?

The range of data collected can be controlled. In accordance with the principle of data saving, only those data required for the purpose of the targeted reports are stored for each data subject, and only as long as they are required.

Data is basically used in target reports where we display aggregate business metrics (KPIs).

Due to the above, the potential risk of private use has occurred and any negative impact thereof has been minimized.

Can you offer individuals an opt-out? Yes / No

MAKING THE DECISION

This is where you use your answers to Parts 1, 2 and 3 to decide whether or not you can apply the legitimate interests basis.

Can you rely on legitimate interests for this processing? Yes / No

Do you have any comments to justify your answer? (optional)

LIA completed by: Dr. Tamás Forgács, CISA, CISM Date: 2019.04.09

WHAT'S NEXT?

Keep a record of this LIA, and keep it under review.
Do a DPIA if necessary.
Include details of your purposes and lawful basis for processing in your privacy information, including an outline of your legitimate interests.

ISO 27001 CERTIFICATE