Data Protection Policy

1. Regarding the activity performed based on the Contract, Service Provider (JobCTRL Informatikai Kft.; 1118 Budapest, Rétköz u. 5.; company registration number: 01-09-949636; represented by: Attila Vadász 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

30 April 2020

Attila Vadász

JobCTRL Informatikai Kft.

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 3 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. 5.; registration number: 01-09-949636; represented by: Attila Vadász 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 5.; registration number: 01-09-937541; represented by: Attila Vadász)

	INPHONE Kft. (1118 Budapest, Rétköz utca 5.; 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).