Bulgaria Staff Data Protection Policy

Last updated May 2018

Part A of this Policy sets out how Fourth processes staff data in accordance with data protection laws.

Part B of this Policy sets out the key things Fourth asks staff to do to ensure that Fourth does in fact comply with its data protection obligations.

The Schedule to this Policy sets out Fourth's Bulgaria Staff Data Retention Policy.

PART A - How Fourth processes staff data in accordance with data protection laws

We are committed to complying with all relevant data protection laws. The proper treatment of personal data is integral to our success as a business and to maintaining trust of the people we deal with.

As a general approach, we are accountable for and demonstrate compliance with our data protection obligations by:

- Conducting Privacy Impact Assessments where necessary and adapting and improving our processes and procedures to address any risks.
- Regularly reviewing and updating internal data protection policies, privacy notices, and information security policies as appropriate.
- Conducting relevant and tailored staff training when staff join the company and ensuring staff are informed about Fourth's data protection obligations and their role in upholding these obligations; and
- Appointing a Data Protection Officer ("**DPO**"), contact details for whom are set out at the end of this Part A.

1 We process data fairly and lawfully and in a transparent manner.

Политика за защита на личните данни на служителите във Форт България

Последна актуализация май 2018г.

Раздел А от тази Политика урежда начина, по който Форт обработва данни на служителите съгласно правилата за защита на лични данни.
Раздел Б от тази Политика урежда ключовите неща, които Форт изисква от служителите да направят, за да може Форт да осигури действителното съблюдаване на задълженията за защита на лични данни.
Приложението към тази Политика съдържа Политика за съхранение на данни на служителите на Форт в България.

РАЗДЕЛ А – как Форт обработва данни на служителите в съответствие с правилата за защита на лични данни

Основна цел за нас е да спазваме всички правила, свързани със защитата на лични данни. Правилното третиране на лични данни е изключително важно за нашия успешен бизнес и за поддържането на доверие у хората, с които работим.
Като общ подход, ние сме отговорни и демонстрираме спазването на нашите задължения за защита на лични данни, като:

- Извършваме Оценки на въздействието върху защитата на лични данни при необходимост и адаптираме и подобряваме нашите процеси и процедури, за да можем да адресираме всеки риск.
- Често извършваме прегледи и актуализираме нашите вътрешни политики за защита на лични данни, политики за поверителност и политики за сигурност на информацията при необходимост.
- Провеждаме подходящо и индивидуално обучение на служителите при постъпване на нов служител в дружеството и информираме служителите относно задълженията на Форт за защита на лични данни и тяхната роля за подпомагането на изпълнението на тези задължения; и
- Избор на Длъжностно лице за защита на данните („**ДЛЗД**"), чиито данни за контакт са поместени в края на Раздел А.

1 Ние обработваме лични данни добросъвестно, законосъобразно и по прозрачен начин.

Please see our Bulgaria Staff Privacy Notice (available on Engage) for full and specific information on how we process staff data. We keep this notice up to date to comply with our obligations of fair processing and transparency. We also allow individuals to monitor the processing of their data and keep their data up to date by allowing them to see and edit their online basic HR information through People System.

2 We process data for specific, explicit and legitimate purposes and do not further process data in a manner that is inconsistent with those purposes.

We only process staff data for the reasons set out in the Bulgaria Staff Privacy Notice. If we ever need to use staff data for any other reason than those already communicated to staff we will ensure that we communicate those purposes to staff before we do so.

3 We keep adequate data, which is relevant and limited to what is necessary for the purpose.

We do not collect data in excess of what we need for the purposes set out in our Bulgaria Staff Privacy Notice and achieve this through:

- training People Ops to only collect data which is needed for the purposes we have set out in the Bulgaria Staff Privacy Notice;
- following our Bulgaria Staff Data Retention Policy, which People Ops are trained on, which helps to limit the staff data we retain, which can be found in the Schedule to this Policy; and
- maintaining relevant documentation on our processing activities which allows us to easily review and what data we are processing and take active steps to reduce data down to only what is needed for the business;
- conducting audits of the data Fourth collects and processes; and

Моля вижте нашата Политика за поверителност за служителите в България (достъпна в Engage) за цялостна и детайлна информация затова как обработваме данните на служителите. Поддържаме тази политика актуална, за да спазим задълженията си за добросъвестност при обработването и за прозрачност. Ние позволяваме лицата да следят обработването на техните данни и да поддържат данните си актуални, като им даваме възможност да виждат и да коригират тяхната основна информация, събирана от Човешки ресурси онлайн чрез People System.

2 Ние обработваме данни за конкретни, изрично указани и легитимни цели и не ги обработваме по начин, който е несъвместим с тези цели.

Обработваме данни на служителите за целите, посочени в Политиката за поверителност за персонала в България. Ако се наложи да използваме данни на служителите за други цели, различни от тези, за които сме уведомили служителите, то ние ще ги уведомим и за новите цели, преди да започнем да обработваме данните.

3 Ние съхраняваме подходящи данни, свързани с и ограничени до необходимото във връзка с целта, за която се обработват.

Не събираме данни, извън тези, които са ни необходими за целите, посочени в нашата Политика за поверителност за служителите в България и постигаме това като:

- обучаваме служителите от People Ops единствено да събират данни, които са необходими за целите, посочени в Политиката за поверителност за служителите в България
- спазваме нашата Политика за съхранение на данни за служителите в България, на база на която са обучавани служителите от People Ops, което помага за ограничаване на данните на служителите, които съхраняваме, като Политиката се съдържа в Приложение към тази Политика; и
- поддържаме документация, свързана с нашите дейности по обработване, която спомага за улесняване преглеждането на това какви данни обработваме и за предприемането на активни стъпки за намаляване на данните единствено до тези, които са необходими за бизнеса;
- извършване на одити относно данните, които Форт събира и обработва; и

- conducting reviews of our company forms and other data collection methods to ensure there are no fields which collect excessive and unnecessary information.

4 We endeavour to keep all personal data accurate and, where necessary, kept up to date.

We keep data up to date by asking staff in our Bulgaria Staff Privacy Notice and Part B of this Policy to keep People Ops informed of any changes in their personal data or to update their personal data themselves on People System where possible. People Ops also, through People System and the N, Drive, continually monitor the data we hold and consider what data may be out of date and take steps (usually by contacting the member of staff) to update that information to correct it. People Ops also conduct data audits from time to time, and the accuracy of data will be considered and checked as part of those audits.

5 We keep data in a form which permits identification of the data subject for no longer than necessary for the purpose.

We anonymise staff personal data where necessary and apply retention periods in accordance with our Bulgaria Staff Data Retention Policy (which can be found in the Schedule to this Policy).

6 We keep personal data secure and protect it against unauthorised or unlawful processing and against accidental loss, destruction or damage.

We conduct Privacy Impact Assessments as necessary to assess and improve our compliance efforts.

We store employee data mostly on People System, on the N, U and V Drive and in Microsoft Exchange 365:

- People System is restricted to use by People Ops teams in our offices around the world who can see the personal data of all staff. Staff who access People System can only see their own personal data and that of their team if they are a manager.

- извършване на прегледи на нашите формуляри и на другите начини за събиране на данни, за да осигурим, че не се събира излишна или ненужна информация.

4 Ние полагаме усилия, за да поддържаме всички лични данни точни и при необходимост в актуален вид.

Поддържаме данните в актуален вид, като изискваме от служителите в нашата Политика за поверителност на служителите в България и Раздел Б от тази Политика да информират служителите от People Ops за всякакви промени в личните им данни или сами да актуализират личните си данни на People System, ако е възможно. Служителите от People Ops също чрез People System и N, Drive непрекъснато следят данните, които съхраняваме и преценяват какви данни може да са неактуални и предприемат стъпки (обикновено като се свързват със служител) за актуализиране на информацията, за коригирането й. Служителите от People Ops също понякога извършват одити на данните и точността на данните се проверява като част от тези одити.

5 Съхраняваме данните във форма, която позволява идентифицирането на субекта на данни за период, не по-дълъг от необходимото за целта.

Ние анонимизираме данните на служителите, когато е необходимо и ги съхраняваме за определени срокове съгласно нашата Политика за съхранение на данни на служителите в България (която е поместена в Приложение към тази Политика).

6 Осигуряваме подходящо ниво на сигурност на личните данни и защита срещу неразрешено или незаконосъобразно обработване и срещу случайна загуба, унищожаване или повреждане.

Извършваме Оценка на въздействието върху защитата на личните данни при необходимост, за да оценим и подобрим нашите усилия за спазване на задълженията ни.

Съхраняваме данни за служителите предимно на People System, на N, U и V Drive и на Microsoft Exchange 365:

- People System може да бъде използвана само от екипите на People Ops, разположени в офисите ни по света, които могат да виждат личните данни на всички служители. Служителите, които имат достъп до People System могат единствено да

- N Drive is restricted to use by People Ops teams only in our offices around the world who can see the personal data of all staff.
- U and V Drive is restricted to use by People Ops and Finance teams only in our offices around the world who can see the personal data of all staff.

- Microsoft Outlook will store employee data which is contained in emails which will be available to those people emails are sent to, received by and copied on. Occasionally the IT teams may access these systems also for security purposes and in accordance with our IT Security policies (available on Engage). Occasionally People Ops may request access to members of staff's Microsoft Outlook systems, for example, as part of internal investigations (such as for grievance or disciplinary purposes).

We utilise many different security features which are created and improved on an ongoing basis, which currently include:

- Segregating personal data from other networks, by keeping personal data all in the following programs: People System, the N Drive and Salesforce. This enables us to add extra security features to prevent hacking and loss of data such as utilising Access Control Lists, Web Application Firewalls and security event logging;

- Keeping information security policies up to data and ensuring that staff are trained on these;

- Installing and keeping updated boundary firewalls and Internet gateways;

- Monitoring of network traffic for suspicious activity;

- Installing software updates to mitigate against known vulnerabilities;

- Installing and keeping updated anti-malware products on client machines and ensuring they are active;

виждат своите лични данни и тези на своите екипи, ако са мениджъри.
- N Drive може да се използва само от екипите на People Ops в офисите ни по света, които могат да виждат личните данни на всички служители.
- U и V Drive може да се използва само от екипите на People Ops и Финанси само от нашите офиси по света, които могат да виждат личните данни на всички служители.
- Microsoft Outlook ще съхранява данни на служителите, които се съдържат в имейли, които ще са достъпни до лицата, до които са изпратени, получени или копирани имейлите. Понякога ИТ екипи може да имат достъп до тези системи за целите на сигурността и съгласно нашите Политики за ИТ сигурност (достъпни на Engage). Понякога служителите от People Ops може да поискат достъп до системите на Microsoft Outlook, например като част от вътрешни проверки (при оплаквания или с дисциплинарни цели).

Използваме разнообразни защитни елементи, които се създават и подобряват постоянно и които в настоящия момент включват:

- Отделяне на лични данни от други мрежи като всички лични данни се съхраняват в следните програми: People System, N Drive и Salesforce. Това ни позволява да добавяме допълнителни защитни елементи, за да предотвратим хакване и загуба на данни, като използване на Списъци за контрол на достъпа, Защитни стени за уеб приложения и регистриране на събития със защитни цели;
- Поддържане на политиките за защита на информацията актуални и гарантиране обучаването на служителите по тях;
- Инсталиране и поддържане на актуализирани гранични защитни стени и Интернет портали;
- Следене на мрежовия трафик за подозрителни действия;

- Инсталиране на софтуер ъпдейти за намаляване на опасността от познати рискове;
- Инсталиране и поддържане на актуални продукти срещу зловредни кодове на машините на клиентите и гарантиране, че са активни;

- Removing unused software and services from our devices regularly to reduce the number of vulnerabilities;
- Enforcing the use of strong passwords across all systems;
- Ensuring that default passwords used by software or hardware are changed when implementing systems;
- Encryption of mobile devices taken outside of the workplace;
- Encrypting of individual files prior to transmission where they contain particularly sensitive data;
- Ensuring that all mobile devices have a remote disable or wipe facility to allow us to securely delete all data in the event of loss or theft;
- Using electronic access cards in order to control and log who enters the building, who enters specifically Fourth office space and who enters IT control/server rooms;
- Highly restricted and authorised access only to data centres containing People System data;
- Using user authentication to log into locations containing personal data, and only allowing limited people access at all. Users only have access to an account with permissions appropriate to the job they are carrying out;
- Storing People System information on encrypted storage.

For any hard copy document which contains staff personal data (such as employment contracts, copies of doctor's notes etc) one hard copy is provided to the staff member and another hard copy is provided to a payroll company which operates as Fourth's data processor regarding the employees' hard copy dossiers.

7 We will also process data in line with individuals' rights and will not transfer data to people or organisations situated in countries without adequate protection.

- Редовно премахване на неизползван софтуер и услуги от нашите устройства за намаляване на рисковете;
- Налагане на използването на надеждни пароли по всички системи;
- Осигуряване на смяната на стандартните пароли при въвеждането на системите;
- Кодиране на мобилните устройства, когато се изнасят извън работното място;
- Кодиране на индивидуални файлове преди прехвърляне, ако съдържат чувствителни данни;
- Гарантиране, че всички мобилни устройства разполагат с устройство за дезактивиране или почистване от разстояние, което ни позволява безопасно да изтрием всички данни в случай на загуба или кражба;
- Използване на електронни карти за достъп за контрол и регистриране на влизащите в сградата, на влизащите специално в офисното пространство на Форт и на тези, които влизат в ИТ контролни/сървърни стаи;
- Силно ограничен и подлежащ на разрешение достъп до центровете за данни, съдържащи данни от People System;
- Идентифициране на потребители за влизане в места, съдържащи лични данни и предоставяне на достъп само на ограничен кръг от лица. Потребителите имат достъп само до профил след разрешения, съответстващи на извършваната от тях работа;
- Съхраняване на информацията от People System в кодирани хранилища.

За всеки документ на хартия, който съдържа лични данни на служители (като трудови договори, копия на бележки, издадени от лекари и т.н.) един документ се предоставя на служителя и друг на дружеството, което администрира заплатите, което действа като обработващ на данните на Форт що се отнася до досиетата на хартия на служителите.

7 Ние ще обработваме данни, спазвайки правата на лицата и няма да прехвърляме данни на хора или организации, намиращи се в държави, в които не е осигурено адекватно ниво на защита.

We inform staff of their rights in our Bulgaria Staff Privacy Notice (available on Fourth Engage). We only send data to other countries where the data is adequately protected, as set out in our Bulgaria Staff Privacy Notice.

If you consider that we are in breach of the terms of this policy, you should raise the matter with the DPO. The DPO is responsible for ensuring compliance with the Act and with this Policy. Any questions about the operation of this Policy should be referred in the first instance to the DPO.

CONTACT DETAILS

If you have any questions, please contact Paul Cocker (Data Protection Officer) at:
Address: 90 Long Acre, Covent Garden, London WC2E 9RA, UK
E-mail: security@fourth.com

Our Bulgaria Staff Privacy Notice is available on Engage if you would like further information about our data protection obligations towards staff.

This Policy may be updated as necessary from time to time and does not form part of any contract of employment or other contract to provide services.

PART B - Key things Fourth staff must do to ensure Fourth's compliance with its data protection obligations

1. **Do not collect excessive data or use information on customer's employees for unexpected purposes.** If you are processing data you would not usually expect to process, or are processing data for different reasons than you would normally, talk to the data protection representative.

2. **Help us keep our records up to date** (both your information on People System as well as customer information)**.**

3. **Ensure that the correct on-boarding process is used for customers** so that they receive the appropriate information about how their data will be used and the correct contracts are put in place.

Ние информираме служителите за техните права в нашата Политика за поверителност за служители в България (достъпна на Fourth Engage). Изпращаме данни до други държави само когато данните са надеждно защитени, както е посочено в нашата Политика за поверителност за служители в България.
Ако сметнете, че нарушаваме правилата на тази политика, трябва да повдигнете въпроса пред ДЛЗД. ДЛЗД е отговорно за осигуряването на спазването на законодателството и на тази Политика. Всякакви въпроси относно приложението на тази Политика трябва да се отнасят като първа инстанция до ДЛЗД.

ДАННИ ЗА КОНТАКТ

Ако имате въпроси, моля свържете се с Пол Кокър (Лице за защита на данните) на:
Адрес: Лонг Акър 90, Ковънт Гарден, Лондон, WC2E 9RA, Великобритания
Имейл: security@fourth.com

Нашата Политика за поверителност на служителите в България е достъпна на Engage, ако желаете допълнителна информация за нашите задължения към служителите във връзка със защитата на данните им.
Тази Политика може да бъде актуализирана при необходимост от време на време и не е част от трудови договори или други договори за предоставяне на услуги.

РАЗДЕЛ Б – ключови неща, които служителите на Форт трябва да правят, за да се осигури спазването на задълженията за защита на данните от страна на Форт

1 **Не събирайте излишни данни или не използвайте информация за служители на клиенти за неочаквани цели**. Ако обработвате данни, които обикновено не очаквате да обработвате или ако обработвате данни за различни от обикновено цели, говорете с представителя за защита на данни.

2 **Помогнете ни да поддържаме регистрите ни** в актуален вид (информацията за Вас, намираща се на People System и информацията за клиенти).

3 **Осигурете, че се използва правилният процес по въвеждане на клиенти в процеса на работа**, така че клиентите да получат подходяща информация затова как данните им ще бъдат използвани и че ще бъдат сключени съответните договори.

4. **Be mindful who you share information with:**

- Fourth's Group Companies: You may share personal data we hold with any other Fourth entity, which means any branch of the company, our subsidiaries, our ultimate holding company and its subsidiaries, including: Fourth USA, Fourth Bulgaria EOOD, Fourth Software Trading LLC.

- Third parties: Where we share information with (or receive information from) third parties we must ensure that we have data processing agreements in place in order to protect the security of this data. Please contact the DPO if you are unsure whether you can share or receive information.

- Recipients outside the European Economic Area and other approved locations: We are prevented under data protection laws from transferring any personal data we hold to a country outside the European Economic Area or other approved locations unless we comply with certain conditions. If you need to transfer data outside of these areas, please contact the DPO.

5. **Comply with our Information and Security policies**, which are available on Engage, including in particular:

- using secure methods of transmission of data, for example, SFTP rather than FTP or HTTPS links rather than HTTP links if you are sending personal data outside of Fourth;

- ensuring that all personal data is encrypted, for example, using password protection when sending personal data by email outside of Fourth, and sending that password via a different medium;

- using anti-malware software (AVG/Webroot) to check files from the Internet, email attachments from

4 **Внимавайте с кого споделяте информация:**

- Дружества от групата на Форт: може да споделяте лични данни, които съхраняваме с всяко друго дружество на Форт, което означава всеки клон на дружеството, нашите дъщерни дружества, нашето дружество-майка и неговите дъщерни дружества, включително: Форт САЩ, Форт България ЕООД, Форт Софтуер Трейдинг ООД.
- Трети лица: Когато споделяме информация с (или получаваме информация от) трети лица, трябва да осигурим, че разполагаме с договори за обработване на данни, за да осигурим сигурността на тези данни. Моля свържете се с ДЛЗД, ако не сте сигурни дали можете да споделите или да получите информация.
- Получатели извън Европейското икономическо пространство и други одобрени локации: не можем по силата на законодателството за защита на лични данни да прехвърляме всякакви лични данни на страна извън Европейското икономическо пространство или други одобрени локации освен ако не спазим определени условия. Ако искате да прехвърлите данни извън тези локации, моля свържете се с ДЛЗД.

5 **Спазвайте нашите Политики за защита на информацията**, които са достъпни на Engage, включително:

- използване на защитни механизми за прехвърляне на данни, например SFTP вместо FTP или HTTPS връзки вместо HTTP връзки, ако изпращате лични данни извън Форт;

- гарантиране, че всички лични данни са кодирани, например, използване на защита чрез пароли, когато се използват лични данни чрез имейл извън Форт и изпращане на паролата по различен начин;
- използване на софтуер за откриване на зловреден софтуер (AVG/Webroot), за да проверите

outsiders and disks from non-Fourth sources before opening or downloading;

- notifying the IT team if you suspect that any virus has been introduced to the Fourth network;
- be mindful of the risks of using open (unsecured) wireless networks (such as Internet cafes or public libraries) or making calls in public places or around people without a need-to-know;
- grant access to confidential information on a need-to-know basis, and only with the approval of the data owner;
- report any and all information risks to the Head of Security & Compliance; and
- do not access any rooms, network or network services which you have not been authorised to access.

6. **Report any data security breaches you discover to the Data Protection Officer immediately.** Guidance of what a data security breach might look like is included in our Information and Security Policies.

Pass any requests from customers or other employees about their personal data to the Data Protection Officer immediately.

SCHEDULE

Bulgaria Staff Data Retention Policy

Last updated May 2018

A. Purpose

This Bulgaria Staff Data Retention Policy sets out how Fourth operates in relation to data storage, retention and destruction, including the default and other retention periods applicable to Bulgaria Staff data that Fourth possesses.

файловете от Интернет, прикачените файлове в имейлите, които получавате от външни лица и дискове от източници извън Форт преди да отворите или свалите файла;

- уведомяване на ИТ екипа, ако имате подозрения, че има вирус в мрежата на Форт;
- внимавайте относно рисковете при използване на отворени (незащитени) мрежи (като интернет кафета или публични библиотеки) или при обаждания в публични места или покрай хора, за които принципът необходимост да знаят не е налице;
- давайте достъп до конфиденциална информация при спазване на принципа необходимост да се знае и само с одобрението на притежателя на данните;
- докладвайте за всякакви рискове за информацията на Ръководителя на отдел „Сигурност и Изпълнение“; и
- Не влизайте в стаи, мрежи или мрежови услуги, за които нямате разрешение за достъп.

6 **Незабавно докладвайте всякакви нарушения на сигурността на данните на Длъжностно лице за защита на данните**. Описание на това какво представлява нарушение на сигурността на данните е включено в Политиките за информация и сигурност.

Незабавно предавайте всякакви искания от клиенти или други служители относно техните лични данни на Длъжностното лице за защита на данните.

ПРИЛОЖЕНИЕ

Политика за съхранение на данните на служителите в България

Последна актуализация май 2018 г.

А. Цел

Тази Политика за съхранение на данните на служители в България определя как Форт действа във връзка със запзване на данните, съхраняване и унищожаване, включително началният и други периоди на съхранение, които са приложими за данните на служителите в България, които Форт обработва.

We will keep staff data in a form which permits staff identification for no longer than is necessary for the purposes for which the personal data is processed. We have assessed those periods having considered Fourth's need to satisfy any legal, accounting, or reporting requirements (see our Bulgaria Staff Privacy Notice for more information on the purposes for which staff data is processed) as well as the practicalities of us effectively deleting such data from our systems.

Ще съхраняваме данни за служителите по начин, който позволява идентифициране на служителите за толкова, за колкото е необходимо за целите, за които личните данни се обработват. При преценката на тези периоди взехме предвид необходимостта Форт да задоволи всяко правно, счетоводно или отчетно изискване (вижте нашата Политика за поверителност за служители в България за повече информация за целите, за които данните на служителите се обработват), както и възможността на практика ефективно да можем да изтрием тези данни от нашите системи.

B. Retention periods for employment documents containing personal data

Б. Периоди на съхранение на трудови документи, съдържащи лични данни

Category/ Категория	**Type of information/ Вид информация**	**Default Retention Period/ Предвиден период на съхранение**
1	1. employment agreements/трудови договори; 2. orders for re-appointment to another position within the company/заповеди за преназначаване на друга длъжност в дружеството; 3. orders approving the use of more than 30 business days of unpaid leave per year/ заповеди, с които се разрешава ползването на повече от 30 работни дни неплатен отпуск в рамките на една година; 4. orders for the termination of the employment agreement/ заповед за прекратяване на трудовия договор; 5. labour books of employees/трудови книжки на служителите; 6. certificates used to prove length of service (the so called *удостоверения обр. УП-1, обр. УП-2, обр. УП-3, обр. 30)/ удостоверения за трудов стаж (удостоверения обр. УП-1, обр. УП-2, обр. УП-3, обр. 30);* 7. protocols for approved and paid remunerations while the employer has been within an insolvency procedure/ протоколи за одобрени и платени възнаграждения, докато работодателят е в открито производство по несъстоятелност; 8. other documents that would allow the estimation of the employee's length of service, the received income, the category of work, etc./други документи, от които е виден трудовият стаж на служителите, полученият доход, категориите труд и други; 9. payment orders for the payment of remunerations via bank transfers/платежни нареждания за превеждане на възнаграждения по банков път;	50 years from the end of the applicable tax year in which termination date occurs/ 50 години от края на приложимата финансова година, през която се прекратява трудовото правоотношение

	10. any payroll documents that prove the calculation and the payment of the employee's remunerations/ ведомости, които доказват изчисляването и заплащането на възнагражденията на служителите.	
2	Any other personal data and documents not falling under point 1 and related to the employment agreement/всякакви други лични данни и документи, които не попадат в точка 1 и които са свързани с трудовото правоотношение.	3 from the end of the applicable tax year in which termination date occurs /3 години от прекратяването години от края на приложимата финансова година, през която се прекратява трудовото правоотношение

C. Staff data stored on People System

Bulgaria staff electronic data is processed by Fourth and stored on People System (which is an internal HR version of the Fourth Solution). Both People Ops and staff themselves can upload and edit data on People System.

People System has default periods for which certain data is retained which are set to the default periods listed below, after consideration of the statutory retention periods required for each set of data.

В. Данни на служителите, съхранявана на People System

Данните в електронен вариант на служителите в България се обработват от Форт и се съхраняват на People System (която е вътрешна версия на Fourth Solution, която се използва от Човешки ресурси). И служителите от People Ops, и самите служители могат да качват и коригират данните, поместени на People System.

People System има зададени периоди на съхранение на различните данни, които са определени съгласно зададените периоди по-долу, след като са взети предвид задължителните периоди на съхранение за всеки вид данни.

Category /Категория	**Type of information/ Вид информация**	**Default Retention Period/Зададени периоди на съхранение**
1	- Staff basic information (names, birth date, address, nationality, gender, etc)/Основна информация за служителите (имена, дата на раждане, адрес, националност, пол, други); - Yearly gross salary data/Годишни данни за брутните заплати; - Holiday records/ Отпуски; - Job position in the company; Длъжност в дружеството; - Start date / Resignation date/ Дата на постъпване на работа/ дата на прекратяване на трудовото правоотношение; - Reason for resignation/ Основание за прекратяване на трудовото правоотношение	3 years from the end of the applicable tax year in which termination date occurs / 3 години от края на приложимата финансова година, през която се прекратява трудовото правоотношение

D. Staff data held on the N, U and V Drive and other places

People Ops and Finance also store staff data electronically on the N Drive. Only People Ops can view and edit data on N Drive and only Finance can view data on the V drive, both can view data on the U drive as the Drives do not have an in-built automated system of deleting your data, People Ops and Finance will delete all members of staff's personal data stored on the Drive following 3 years/ 50 years from the end of the applicable tax year in which termination date occurs, whichever term applies. When staff leave the company their personal data stored on the Drives is filed into a specific folder relating to the month and year they terminated in order to facilitate easy and complete deletion by People Ops and Finance at the appropriate time.

Personal data about you stored on Salesforce (in relation to your relationship with customers), will be retained for the duration of our ongoing relationship with the customer and we will delete data about you on Salesforce in relation to particular customers as and when we remove the customer from Salesforce.

Staff personal data will also be deleted from the following places:

- CCTV videos hosted by the building security team will not be requested or accessed by Fourth;
- access card information which is collated and held by the security team on computers within the building; and
- computer logs in terms of your use of Internet sites etc.

All such data under points 2 and 3 will also be anonymised or deleted after 3 years from the end of the applicable tax year in which termination date occurs / or will not be accessed by Fourth after data 3years from the end of the applicable tax year in which termination date occurs and will be deleted in accordance with the service provider's retention procedures where applicable. Data from CCTV videos will be retained for a period of two months as per the Bulgarian Private Security Act.

Г. Данни на служителите, които се съхраняват на N, U и V Drive и на други места

Служителите в People Ops и Финанси също съхраняват електронни данни на N Drive. Само служителите от People Ops може да виждат и поправят данни на N Drive и само Финанси могат да виждат данни, съхранявани на V drive, като служителите и от двата отдела могат да виждат данни на U drive, като Drives нямат вътрешно-автоматизирана система за изтриване на Вашите данни, служителите от People Ops и Финанси ще изтриват личните данни на служителите, съхранявани на Drive след изтичането на 3 години/50 години от края на съответната финансова година, в която е настъпило прекратяването на трудовото правоотношение, който срок е приложим. Когато служител напусне дружеството, личните му данни, съхранявани на Drives се пренасят в специална папка, свързана с месеца и годината, в която е настъпило прекратяването, за да се улесни и извърши изтриването от служителите на People Ops и Финанси при изтичане на съответния срок.

Лични данни за Вас, съхранявани на Salesforce (във връзка с вашата връзка с клиенти) ще се съхраняват за срока, докато взаимоотношения с клиента все още съществуват и ние ще изтрием данните за Вас от Salesforce във връзка с определени клиенти, когато премахнем клиента от Salesforce.

Лични данни на служителите също ще бъдат изтривани от следните места:

- видео записи, направени от екипа, който отговаря за защитата на сградата, няма да могат да бъдат искани от или достъпвани от Форт;
- информация за картите за достъп, която се събира и пази от екипа по сигурността на компютри в сградата; и
- компютърни логове във връзка с използването на интернет сайтове и т.н.

Всички данни по точки 2 и 3 ще бъдат също анонимизирани или изтрити след изтичането на 3 години от края на приложимата финансова година, през която е настъпило прекратяването/ или Форт няма да има достъп до тях след изтичането на 3 години от края на приложимата финансова година, през която е настъпило и прекратяването и ще бъде изтрита съгласно процедурите за съхраняване, предоставени от доставчика на услуги, ако е приложимо. Данните от видео записи ще бъдат съхранявани за срок от 2

	месеца съгласно българския Закон за частната охранителна дейност.
For any hard copy documents which contain your personal data (such as your original employment contract) one hard copy will be provided to the staff member and another hard copy will be provided to a payroll company which operates as Fourth's data processor regarding the employees' hard copy dossiers.	За всеки документ на хартия, който съдържа Ваши лични данни (като например Вашият трудов договор в оригинален екземпляр), един екземпляр на хартия ще бъде предоставен на служителя и друг на дружеството, което се занимава със заплатите и което оперира като обработващ на личните данни на Форт що се отнася до досиетата на служителите, които са на хартия.
From time to time Fourth may change the retention periods and/or introduce additional retention periods to apply to different categories of, or subsets of, staff data. Any such changes will be notified to staff by email and this policy will be updated accordingly. Data will be kept in accordance with the terms of the Bulgaria Staff Data Protection Policy and as detailed in the Bulgaria Staff Privacy Notice.	Понякога Форт може да промени периодите на съхранение и/или да въведе допълнителни периоди на съхранение, които да са приложими към различни категории или подкатегории данни на служителите. Всякакви промени ще бъдат отнесени до знанието на служителите чрез имейл и тази политика ще бъде автоматично актуализирана. Данните ще се съхраняват съгласно условията в Политиката за съхранение на данни на служители в България и както е посочено в Политиката за поверителност за служители в България.
Data that is made anonymous by Fourth may be kept permanently. Fourth will take all appropriate steps to ensure that the data that has been anonymised cannot be re-identified.	Анонимизирани данни от Форт могат да се съхраняват неограничено. Форт ще предприеме подходящи стъпки, за да осигури, че данните са анонимизирани и не могат да бъдат идентифицирани с конкретно лице.
E. Destruction and Disposal	**Д. Унищожаване**
At the expiry of the applicable retention periods referred to at paragraphs B and C above, Fourth will delete the data. The technical means by which Fourth "deletes" staff data are:	След изтичането на приложимите периоди на съхранение, посочени в параграфи Б и В по-горе, Форт ще изтрие данните. Техническите средства, с които Форт „изтрива" данни на служители са:
(a) physical documents will be confidentially destroyed or returned to the staff member;	(а) документите на хартиен носител ще бъдат унищожени или върнати на служителя;
(b) physical disks and media will be subject to a secure wipe prior to reissue and securely disposed of and a certificate obtained when end-of-life;	(б) съдържанието на дисковете или медията ще бъдат надлежно изтрити преди да бъдат преиздадени и освободени по сигурен начин и следва да бъде получено удостоверение при изтичане на срока му;
(c) CDs, DVDs and Blu-ray discs will be destroyed;	(в) CD-та, DVD-та и Blu-ray дискове ще бъдат унищожавани;
(d) virtual documents will be deleted as far as practically possible;	(г)виртуални документи ще бъдат изтривани, доколкото е практически възможно;
(e) personal data within databases (i.e. People System) will be overwritten;	(д) лични данни в бази данни (например People System) ще бъдат надписани;
(f) personal data held electronically will be converted to a scrambling script which makes data unreadable, or will be anonymised; and	(е) лични данни, съхранявани електронно ще бъдат конвертирани в скрипт, който прави данните нечетими или ще бъдат анонимизирани; и

(g) personal data within backups will be phased out through rotation.

F. Limitations

Fourth will delete the personal data, in accordance with its normal backup cycle and whilst this may be deleted immediately, archive copies may remain for up to 13 months after the data of deletion, either on its live platform or as part of its standard backup and archiving procedures.

G. Contact Details

If you have any questions, please contact Paul Cocker (Data Protection Officer) at:
Address: 90 Long Acre, Covent Garden, London WC2E 9RA, UK
E-mail: security@fourth.com

The present Notice was prepared in two identical originals in English and in Bulgarian – one for each Party. In case of discrepancies between the Bulgarian and the English versions, the Bulgarian version shall prevail.

(ж) лични данни от архивите ще бъдат премахвани постепенно на ротационен принцип.

Е. Ограничения

Форт ще изтрие личните данни, съгласно нормалния архивен процес и ако това може да стане веднага, то архивни копия може да бъдат съхранявани до 13 месеца от датата на изтриването или на платформа за действащи актове или като част от стандартната процедура по архивиране.

Ж. Данни за контакт

Ако имате въпроси, моля свържете се с Пол Кокър (Длъжностно лице по защита на данните) на:
Адрес: 90 Лонг Акър, Ковънт Гарден, Лондон WC2E 9RA, Великобритания
Имейл: security@fourth.com

Настоящата Политика се изготви в два еднообразни екземпляра на английски и на български език - по един за всяка от Страните. В случай на противоречие между българската и английската версии, с предимство ще се ползва текстът на български език.