Глобална политика на Ipsos
за защита на данните и поверителност
(в сила от 25 май 2018 г.)

Глобална политика на Ipsos за защита на данните и поверителност

Съдържание

1. Въведение 4
2. Обхват 4
3. Прилагане на националните закони и Правилника за поведение 5
4. Принципи за обработка на Лични данни 5
   4.1. Законност, справедливост и прозрачност 6
   4.2. Ограничение на целта 6
   4.3. Минимизиране на данните 6
   4.4. Точност 6
   4.5. Ограничения за съхранение 6
   4.6. Неприкосновеност и поверителност 7
   4.7. Ограничения за изпращане 7
   4.8. Общи мерки и съображения 7
5. Правни основания за обработка на данни 7
   5.1. Данни на респондента 7
      5.1.1. Съгласие с обработката на данни 7
      5.1.2. Обработка на данни за договорни отношения 8
      5.1.3. Обработка на данни съгласно правно разрешение 8
      5.1.4. Обработка на данни при законен интерес 8
      5.1.5. Обработка на специални категории Лични данни 8
      5.1.6. Потребителски данни и Интернет 9
   5.2. Лични данни, предоставени от клиенти 9
   5.3. Данни на служителите 10
      5.3.1. Обработка на данни във връзка с трудовите взаимоотношения 10
      5.3.2. Обработка на данни съгласно правно разрешение 10
      5.3.3. Колективни споразумения за обработка на данни 10
      5.3.4. Съгласие с обработката на данни 11
      5.3.5. Обработка на данни по силата на законен интерес 11
      5.3.6. Обработка на специални категории лични данни 11
      5.3.7. Автоматизирани решения 11
      5.3.8. Телекомуникации и интернет 12
   5.4. Маркетингови контакти 12
6. Изпращане на лични данни 13

7. Обработка на данни от външни доставчици/трети страни 14
8. Права на Субекта на данни 15
9. Поверителност на обработката 15
10. Поверителност на етапа на проектирането и по подразбиране 16
11. Сигурност на обработката 16
12. Одит на защитата на данните 17
13. Инциденти, свързани със защитата на данните 17
14. Отговорности и санкции 18
14.1. Управление 18
14.2. Служители по защита на данните (DPOs) 18
14.3. Главен служител по защита на личната информация на глобално ниво 19
15. Дерогация 19
16. Речник 20
Администратор на данни/Администратор/Съвместен администратор 20
Потребители на данни 20
Обработващ данни или Обработчик 20
Субекти на данни 20
Лични данни 20
Обработване 21
Специални категории данни (p/k/a лични чувствителни данни) 21
Анонимни данни 22
Псевдонимизация 22
PII или Лично разпознаваема информация 22
PHI или Защитена здравна информация 23
PSI или Лична чувствителна информация 23

1. Въведение

Като част от своята социална отговорност, Ipsos се ангажира със спазване на международно ниво на законите, разпоредбите и правилата за защита на данните. Тази политика за защита на данните ("**Политика**" или "**Политика за защита на данните**") се прилага в световен мащаб за Ipsos Group и се базира на приетите на глобално ниво основни принципи за защита на данните. Тази политика възприема основните принципи на Общия регламент за защита на данните ("**GDPR**") на Европейския съюз като минимален стандарт, към който Ipsos Group, нейните служители и доставчици ще трябва да се придържат.

Ipsos зависи от събирането и анализа на информация за реални хора ("**Субекти на данни**"), за да извършва своите проучвания на пазара и свързаните с тях дейности. Поддържането на доверието на респондентите и обществеността изисква респондентите да не са обект на преки неблагоприятни последици, риск или вреда в резултат на предоставянето на информация за себе си или своите Лични данни (за определение и обяснение на този термин и на други термини, изписани с главна буква, моля вижте раздел „Речник") за обработка за бизнес целите на Ipsos. Информацията може да бъде получена от всяко физическо лице или организация.

За да осъществява своята дейност, Ipsos също трябва да събира и обработва определени видове информация за хората, с които работи. Това включва настоящи, бивши и бъдещи служители, доставчици, клиенти и други, с които може да има комуникация. Освен това може понякога Ipsos да бъде задължена по закон да обработва определени видове Лични данни, за да спази дадени законови изисквания.

Тази Политика описва минималните стандарти за това как трябва да се обработват, събират, третират и съхраняват Личните данни, за да отговарят на стандартите на Ipsos за защита на данните.

Потребителите на данни са длъжни да се съобразяват с тази Политика при обработката на Лични данни от името на Ipsos. Всяко нарушение на тази Политика може да доведе до дисциплинарни действия, до и включително уволнение от Ipsos.

2. Обхват

Политиката е приложима на глобално ниво за всички компании на Ipsos, без значение къде се намират. В рамките на Ipsos тази Политика ще формира минималния стандарт, към който трябва да се придържат всички компании, служители и доставчици на Ipsos, независимо дали GDPR се прилага пряко за конкретна дейност или територия.

Всеки, който работи за Ipsos, носи отговорност да гарантира, че Личните данни се събират, съхраняват и третират по подходящ начин.

Отговорност на всеки е Личните данни се третират и обработват в съответствие с настоящата Политика и нейните принципи за защита на данните.

Ipsos също така очаква нейните доставчици/подизпълнители да спазват принципите, посочени в Политиката.

3. Прилагане на националните закони и Правилника за поведение

Настоящата Политика за защита на данните заимства международно приетите принципи за защита на поверителността, подобрени от GDPR. Тя подпомага и допълва всяко приложимо национално законодателство. Съответните национални закони ще имат предимство в случай на конфликт с тази Политика или ако съдържат по-строги изисквания от тази Политика. Трябва да се спазват всички изисквания за регистрация, уведомяване или докладване за обработката на данни съгласно националните закони. Съдържанието на тази Политика трябва да се съблюдава и при отсъствието на съответно национално законодателство.

Всяка компания от Ipsos Group отговаря за спазването на настоящата Политика за защита на данните и приложимите правни задължения. Ако има причина да се смята, че правните задължения противоречат на задълженията по настоящата Политика за защита на данните, съответната фирма трябва да информира Служителят по защита на данните (DPO) за страната и Главния служител по защита на личната информация (CPO). В случай на противоречие между националното законодателство и Политиката за защита на данните, Ipsos ще работи със съответната компания, за да намери практическо решение, което отговаря на изискванията и удовлетворява целите на настоящата Политика, както и на приложимото законодателство.

Освен към настоящата Политика, за своите дейности по проучване на пазара, Ipsos се придържа към изискванията на Международния кодекс на ICC/ESOMAR за проучвания на пазара, общественото мнение и социални изследвания и анализ на данни, който можете да намерите тук.

4. Принципи за обработка на Лични данни

Всички Лични данни трябва да се обработват правилно, независимо от това как се събират, записват и обработват - на хартия, в компютърен файл, база данни или записани върху друг носител, и за да се гарантира това, има общоприети принципи, както е посочено в Насоките на ОИСР относно Защитата на личния живот и трансграничните потоци лични данни, както и съответни защитни мерки в различните правилници по света, включително в GDPR.

Ipsos разглежда законното и правилно третиране на Личните данни и поддържането на доверието на лицата, с които работи, като жизненоважен компонент от своите бизнес дейности, и се ангажира да действа етично и отговорно по отношение на тези Лични данни и винаги да осигурява висока степен на поверителност и сигурност.

За да покаже тези ангажименти, Ipsos се придържа към принципите, свързани с обработката на Лични данни, съдържащи се в GDPR, които сами по себе си са въплъщение на принципите на ОИСР. Ipsos зачита следните принципи, които са обяснени по-подробно по-долу, във връзка с Личните данни, и те са:

- Обработени справедливо и законно.
- Обработени за ограничени цели и по подходящ начин.
- Адекватни, подходящи и не са прекомерни за съответната цел.
- Точни.
- Не се съхраняват повече от необходимото за целта.
- Обработени в съответствие с правата на Субектите на данни.

- Защитени.
- Не се прехвърлят на хора или организации, намиращи се в други държави, без подходящата защита.

4.1. Законност, справедливост и прозрачност

Личните данни трябва да бъдат обработвани и събирани законно, справедливо и по прозрачен начин спрямо Субекта на данни. Освен това Субектите на данни трябва да бъдат информирани за това как се третират техните данни. По принцип Личните данни трябва да се събират директно от съответното лице. В противен случай трябва да се документира правното основание, на базата на което обработването е оправдано. Трябва да се направи консултация със съответния Служител по защита на данните (DPO) дали е необходимо да се направи Оценка на въздействието върху защитата на данните (DPIA) (виж също отделните насоки относно DPIA, които могат да бъдат намерени в интранет).

4.2. Ограничение на целта

Личните данни трябва да се събират само за конкретни, изрични и законни цели и да не се обработват по начин, който е несъвместим с тези цели. Последващи промени в целта са възможни само в ограничена степен и изискват обосновка и валидиране. Трябва да се направи консултация със съответния Служител по защита на данните (DPO) дали е необходимо да се направи Оценка на въздействието върху защитата на данните (DPIA) (виж също отделните насоки относно DPIA, които могат да бъдат намерени в интранет).

4.3. Минимизиране на данните

Личните данни трябва да бъдат адекватни, уместни и ограничени по отношение на целта, за която се обработват. Трябва да се определи дали и до каква степен обработването на Лични данни е необходимо, за да се постигне целта, за която се извършва обработката. Когато целта позволява и когато съответният разход е пропорционален на преследваната цел, вместо Лични данни трябва да се използват анонимизирани данни.

4.4. Точност

Личните данни трябва да бъдат точни и при необходимост - да се актуализират. Трябва да се предприемат всички разумни стъпки, за да се гарантира, че Личните данни, които са неточни във връзка с целите, за които се обработват, се изтриват или коригират незабавно.

4.5. Ограничения за съхранение

Личните данни не трябва да се съхраняват във форма, която позволява идентифициране на Субектите на данни за период, по-дълъг от необходимия за целта, за която се обработват Личните данни. Ipsos няма да съхранява Лични данни за период, по-дълъг от необходимия за целта или целите, за които са били събрани. Ipsos ще предприеме всички разумни стъпки, за да унищожи или да изтрие от своите системи всички Лични данни, които вече не са необходими.

4.6. Неприкосновеност и поверителност

Личните данни трябва да се обработват по начин, който гарантира необходимата защита на Личните данни, така че те да не могат да бъдат разкрити, разпространени, достъпни или манипулирани. Затова когато е методологично възможно и разходът не е непропорционален на рисковете за Субекта на данните, за обработката трябва да се използват псевдонимизирани данни. ЗАБЕЛЕЖКА: псевдонимизираните данни остават и са Лични данни!

4.7. Ограничения за изпращане

Личните данни не трябва да се изпращат в други държави (дори на други компании от Ipsos в тези държави), които не предлагат съответното ниво на защита. Ipsos въведе различни мерки, за да осигури съответното ниво на защита на обща база (виж също параграф 6 за повече подробности), но въпреки това различните държави могат да имат допълнителни и/или различни изисквания, които трябва да се спазват.

4.8. Общи мерки и съображения

Освен това, по отношение на своите дейности за проучване на пазара, Ipsos спазва Международния кодекс на ICC/ESOMAR за проучвания на пазара, общественото мнение и социални изследвания и анализ на данни, както и Контролния лист за защита на данните на Esomar.

5. Правни основания за обработка на данни

Ipsos ще събира, обработва и използва Лични данни само при следните правни основания, винаги при условие че съответното правно основание съществува съгласно приложимото национално законодателство. Едно от тези правни основания се изисква и ако целта за събиране, обработване и използване на Лични данни трябва да бъде променена спрямо първоначалната цел, освен ако няма ясна съвместимост между първоначалната цел и новата цел. Виж също параграф 4.2 и всички потенциални допълнителни изисквания за съответствие.

5.1. Данни на респондента

Респондентите са най-често срещаните Субекти на данни в дейността на Ipsos. Следователно, правилното третиране на техните Лични данни е в основата на работата на Ipsos.

5.1.1. Съгласие с обработката на данни

Личните данни могат да бъдат обработвани след съгласие от Субекта на данните. Преди да даде съгласието си, Субектът на данни трябва да бъде информиран в съответствие с принципа на прозрачност, посочен в параграф 4.1. За целите на документацията, декларацията за съгласие трябва да бъде получена в писмена форма или по електронен път. В някои обстоятелства, като например при телефонни проучвания, съгласието може

да бъде дадено устно. Във всички случаи даването на съгласие трябва да бъде документирано.

Всяко съгласие е валидно само ако представлява свободно дадено, конкретно, информирано и недвусмислено посочване на желанията на Субекта на данни, с което той като прави декларация или чрез ясни потвърждаващи действия, изразява съгласие за обработката на Личните данни, свързани с него/нея. За указания относно съгласието, моля, вижте ТУК.

5.1.2. Обработка на данни за договорни отношения

Освен съгласието, техните Лични данни могат да бъдат обработени, когато това е необходимо, в контекста на договор, по който Субектите на данни са страна, за да изпълнят съответни задължения и права. Това важи и когато такава обработка е необходима за установяване или прекратяване на договор. Това се отнася по-специално за респондентите (включително тайните купувачи), когато се записват за участие в групи на Ipsos.

Някои държави разглеждат сключването на договор като форма на съгласие.

5.1.3. Обработка на данни съгласно правно разрешение

Обработката на Лични данни също е разрешена, ако националното законодателство изисква, задължава или позволява това. Видът и обхватът на обработката на данни трябва да са необходими за законно разрешената дейност по обработка на данни и трябва да са в съответствие с приложимите законови разпоредби.

5.1.4. Обработка на данни при законен интерес

Личните данни също могат да бъдат обработвани, ако това е необходимо за законните интереси на Ipsos Group и когато националното законодателство предвижда това основание (например чл. 6, ал. 1, буква (e) от GDPR). Правното основание на законния интерес за обработка не се признава във всяка страна, а приложимото национално законодателство има предимство. По принцип специални категории Лични данни не могат да се обработват въз основа на законен интерес! При всички случаи Лични данни не могат да бъдат обработвани въз основа на законен интерес ако в конкретния случай има доказателства, че интересите на Субекта на данни заслужават защита, и че тази защита има предимство. Преди обработването на Лични данни на база законния интерес трябва да се определи дали има интерес, който заслужава защита, и съответната компания от Ipsos Group да направи оценка на законния интерес (под формата на DPIA със специален акцент върху законния интерес). Всяка такава оценка трябва да бъде потвърдена от съответния Служител по защита на данните (DPO) или Главния служител по защита на личната информация (CPO).

5.1.5. Обработка на специални категории Лични данни

Специални категории Лични данни могат да се обработват само ако законът изисква това или ако Субектът на данни е дал своето изрично съгласие. За указания относно съгласието вижте ТУК. Специални категории Лични данни могат също да бъдат обработвани ако са задължителни за уреждане, упражняване или защита на правни искове. В рамките на ЕИП

специални категории Лични данни могат също да бъдат обработвани за научни и исторически изследвания и за статистически цели (чл. 9, ал. 2, буква (й)), при спазване на съответните допълнителни мерки. Преди да се позовете на тези разпоредби, трябва да получите съвет от Служителя по сигурността на данните (DPO) или от Главния служител по защита на личната информация (CPO).

5.1.6. Потребителски данни и Интернет

Ако Личните данни се събират, обработват и използват на уеб сайтове или в приложения, Субектът на данни трябва да бъде информиран за това в декларация за поверителност, включително, ако е приложимо, с информация за "бисквитки" или подобни технически мерки. Декларацията за поверителност и всяка информация за "бисквитки" трябва да бъдат интегрирани така, че да бъдат лесни за идентифициране, пряко достъпни, лесно разбираеми и постоянно на разположение на и за Субекта на данни.

Ако се създават профили на употреба (проследяване), за да се оцени използването на уеб сайтове и приложения, Субектите на данни трябва винаги да бъдат информирани за това в декларацията за поверителност. Проследяване на Субектите на данни онлайн може да се извършва само ако е разрешено от националното законодателство или с изричното съгласие на Субектите на данни. Дори ако проследяването използва псевдоним за Субекта на данните, на Субекта на данните трябва да бъде дадена възможност да се откаже от това в декларацията за поверителност. По отношение на измерването на онлайн аудиторията без предварително съгласие за участие, Ipsos се придържа и към принципите, оповестени от researchchoices.com.

Ако уебсайтове или приложения имат достъп до Лични данни в област, ограничена за регистрирани потребители/респонденти, идентификацията и проверката на Субекта на данни трябва да осигуряват достатъчна защита по време на достъпа.

Като част от ангажимента на Ipsos за придържане към Кодекса на Esomar, правилата и изискванията, предвидени в Ръководството на Esomar за изследване на социалните медии, Ръководството за онлайн изследвания и Ръководството за изследване и анализ на данни с деца, младежи и други уязвими лица, също касаят Ipsos като част от тази Политика.

5.2. Лични данни, предоставени от клиенти

Клиентите доста често изпращат Лични данни на Ipsos. Обикновено това се случва, за да ни предоставят извадки или да допълнят съществуващи извадки. По отношение на получените по този начин Лични данни, Ipsos се явява Администратор и може да обработва тези Лични данни само в съответствие с указанията, договорени с или получени от клиента. Тези указания могат да включват ограничения за изпращане на други страни (включително други компании на Ipsos) или изпращане в други държави, както и специфични изисквания за сигурност. Всички подобни ограничения трябва да бъдат спазени. Задължително е тези инструкции да бъдат документирани в писмен вид и съгласувани, преди съответните договорни споразумения да бъдат приети от Ipsos, за да се гарантира, че Ipsos действително е в състояние да спази всички специфични ограничения или изисквания на клиента.

Независимо от изискванията на клиента, всички предоставени от клиента Лични данни могат само:

а) Да се обработват за целта, за която са предоставени;
б) Да не се съхраняват за период, по-дълъг от необходимия за целта;
в) Да са обект на същите изисквания за сигурност, каквито да приложими към Личните данни на Ipsos.

5.3. Данни на служителите

5.3.1. Обработка на данни във връзка с трудовите взаимоотношения

В трудовите правоотношения Лични данни могат да се обработват когато е необходимо да се започне, да се изпълнява и да се прекрати трудово споразумение. При започване на трудово правоотношение Личните данни на кандидата могат да бъдат обработени. Ако кандидатът бъде отхвърлен, данните му трябва да бъдат изтрити при спазване на изискуемия срок за съхранение, освен ако кандидатът не се е съгласил те да останат в архива за бъдещ процес на подбор. Съгласие е необходимо и за да се използват данните за по-нататъшни процеси на кандидатстване, преди кандидатурите да се споделят с други компании от Ipsos Group.

При съществуващо трудово правоотношение, обработката на данни винаги трябва да се свързва с целта на трудовото споразумение, ако не се прилагат нито едно от следните обстоятелства за разрешената обработка на данни.

Ако в процеса на кандидатстване е необходимо да се събере информация за кандидата от трета страна, трябва да се спазват изискванията на съответните национални закони. В случай на съмнение, трябва да се получи съгласие от Субектите на данните.

Трябва да има законово разрешение за обработката на Лични данни, свързани с трудовото правоотношение, които обаче първоначално не са били част от изпълнението на трудовото споразумение. Това може да включва законови изисквания, колективни разпоредби с представители на служителите, съгласие на служителя или законния интерес на компанията.

5.3.2. Обработка на данни съгласно правно разрешение

Моля, вижте по-горе в параграф 5.1.3 за допълнителните изисквания.

5.3.3. Колективни споразумения за обработка на данни

Ако дейността по обработка на данни превишава целите за изпълнението на даден договор, може да е допустимо, ако е разрешено чрез колективен трудов договор между работодателя и представителите на служителите, в рамките на позволеното съгласно съответното трудово законодателство. Споразуменията трябва да обхващат конкретната цел на планираната по-нататъшна дейност по обработка на данните и трябва да бъдат съставени в рамките на параметрите на националното законодателство за защита на данните и заетостта.

5.3.4. Съгласие с обработката на данни

Данните за служителите могат да се обработват със съгласието на съответното лице. Декларациите за съгласие трябва да бъдат дадени доброволно. В рамките на ЕС/ Европейското икономическо пространство съгласието като цяло не представлява валидно правно основание за обработката в контекста на трудовата заетост, тъй като съществува правна презумпция, че такова съгласие не е дадено доброволно и всяка обработка ще трябва да разчита на някое от другите налични правни основания. Всяко недоброволно съгласие е невалидно. Доколкото съгласието е валидно основание за обработка, вижте допълнителните изисквания по-горе в параграф 5.1.1. Друго усложнение е, че съгласието обикновено може да бъде оттеглено, с което по-нататъшната обработка се предотвратява.

5.3.5. Обработка на данни по силата на законен интерес

Личните данни също могат да се обработват ако е необходимо да се наложи законният интерес на Ipsos Group, където приложимите закони позволяват обработването на Лични данни въз основа на законен интерес. В контекста на трудовата заетост легитимните интереси обикновено са от правно или финансово естество.

Виж по-горе в параграф 5.1.4 за допълнителните изисквания и ограничения на законния интерес.

Контролните или надзорни мерки, които изискват обработка на данните на служителите, могат да бъдат предприети само ако има правно задължение за това или ако има основателна причина. Дори ако има основателна причина, пропорционалността на мерките за контрол също трябва да бъде разгледана преди прилагането на тези мерки. Оправданите интереси на дружеството при осъществяване на контролната мярка (например спазване на вътрешните правила на дружеството или на интересите по отношение на сигурността) трябва да бъдат преценени спрямо интересите, заслужаващи защита, които служителят, засегнат от мярката, може да има при изключването си, а мярката не може да бъде изпълнена, освен ако не бъде счетена за подходяща. Легитимните интереси на дружеството и всички интереси на служителя, заслужаващи защита, трябва да бъдат идентифицирани и документирани, преди да бъдат предприети каквито и да било мерки, чрез законна оценка на интересите. Освен това трябва да се вземат предвид всички допълнителни изисквания, предвидени в националното законодателство (например правата за съвместно вземане на решения на представителите на служителите и правата за предоставяне на информация на Субектите на данни).

5.3.6. Обработка на специални категории лични данни

Специални категории Лични данни могат да бъдат обработвани само ако законът изисква това или ако Субектите на данни са дали своето изрично съгласие. Тези данни могат също да бъдат обработвани ако това е задължително за отстояване, упражняване или защита на правни искове.

5.3.7. Автоматизирани решения

Ако Личните данни се обработват автоматично като част от трудовото правоотношение и конкретни Лични данни се оценяват за вземането на решения (например като част от

процеса на подбор на персонал или оценка на резултатите), тази автоматична обработка не може да бъде единственото основание за решения, които биха имали негативни последствия или създават значителни проблеми за засегнатия служител. За да се избегнат грешни решения, автоматизираният процес трябва да гарантира, че физическо лице оценява съдържанието на ситуацията, и че тази оценка стои в основата на решението. Субектите на данни трябва също да бъдат информирани за фактите и резултатите от автоматизираните индивидуални решения и възможността да отговорят.

5.3.8. Телекомуникации и интернет

Телефонното оборудване, имейл адресите, интранетът и интернетът, заедно с вътрешните социални мрежи, се предоставят от Ipsos основно за задачи, свързани с работата. Те са инструмент и ресурс на компанията. Те могат да се използват в рамките на приложимите законови разпоредби и вътрешнофирмени политики, по-специално на Политиката за сигурност и допустимо използване на информацията. В случай на разрешена употреба за лични цели, трябва да се спазва законът за тайната на телекомуникациите от съответното национално телекомуникационно законодателство, ако е приложимо.

Ipsos използва уеб-филтрираща технология, за да гарантира съответствие със своята Политика за допустимо ползване, измерване и анализ на интернет трафика, другите задължения за спазване на законите и защита от атаки срещу ИТ инфраструктурата или индивидуални потребители. Защитни мерки могат да бъдат приложени за връзките към мрежата на Ipsos, които блокират технически вредно съдържание, и за анализ на моделите на подобни атаки. От съображения за сигурност използването на телефонно оборудване, имейл адреси, интранет/интернет и вътрешни социални мрежи може да бъде заключено постоянно или временно за отделни адреси/местоположения или типове връзки. Оценки на тези данни от дадено лице могат да бъдат направени само при конкретен, обоснован случай на предполагаеми нарушения на законите или на политиките на Ipsos Group, и трябва да бъдат оторизирани от някое от лицата, които могат да разрешат "законно задържане" (виж също Политиката за управление на информационните технологии). Приложимите национални закони трябва да се спазват по същия начин, както и разпоредбите на групата.

5.4. Маркетингови контакти

Като цяло маркетинговите контакти не се различават от респондентите по отношение на защитата на поверителността, която им се предоставя. Техните данни за контакт представляват Лични данни, дори ако са свързани с дейността. Само ако данните за контакт са наистина общи като "contact@acme.com", те не попадат в обхвата на настоящата Политика.

Маркетинговите съобщения често са предмет на специфични правни изисквания, особено ако се изпращат по електронен път или се правят по телефона.

Трябва да се приема, че маркетинговите контакти не са поискали маркетинговите материали. С други думи, получателите не са поискали да получават маркетингови съобщения от Ipsos. За да се процедира законно, условията относно правното основание, и по-специално изискванията за съгласие, предвидени в параграф 5.1.1., се прилагат и тук.

По изключение може да се прилага "soft opt-in" (включване на предишни клиенти), ако са изпълнени следните условия:

- когато данните на Субекта на данни са били получени в хода на продажба или преговори за продажба на услуги на Ipsos;
- когато съобщенията предлагат само подобни услуги; и
- когато на лицето е предоставена лесна възможност да откаже маркетинг при събирането на неговите данни и ако не се откаже в този момент, му се дава лесен начин да направи това във всички бъдещи съобщения.

6. Изпращане на лични данни

Изпращането на Лични данни на получатели извън или в рамките на Ipsos Group е предмет на изискванията за разрешение за обработка на Лични данни съгласно параграф 4.7 Ограничения за изпращане. Получателят на данните (независимо дали е друга компания на Ipsos или подизпълнител) трябва да бъде задължен да използва данните само за определените цели. За външни трансфери изискванията на настоящия параграф и тези от параграф 7 Обработка на данни от външни доставчици/трети страни се прилагат кумулативно.

Ако Лични данни се изпращат на получател извън Ipsos Group до трета държава, този получател трябва да се съгласи писмено да поддържа ниво на защита на данните, еквивалентно на настоящата Политика за защита на данните или съответстващо на изискванията на приложимото законодателство. Например, GDPR предвижда различни изисквания, които трябва да бъдат спазени преди да се стигне до изпращане. Това не се прилага, ако изпращането се прави въз основа на правно задължение. Правно задължение от този вид може да се основава на законите на държавата по местожителство на дружеството от Ipsos Group, изпращащо данните. Като алтернатива, законите на държавата по местожителство на дружеството от Ipsos Group могат да признаят целта на изпращане на данните въз основа на правните задължения на трета държава.

Когато Лични данни се изпращат от трета страна (като доставчик на извадки) на дружество от Ipsos Group, трябва да се гарантира, че Личните данни могат да се използват по предназначение.

Ако Личните данни се изпращат от дружество от Ipsos Group със седалище в една държава до дружество от Ipsos Group със седалище в друга държава, дружеството, внасящо данните, се задължава да съдейства при запитвания, направени от съответния надзорен орган в държавата, в която се намира седалището на страната, изпращаща данните, и да се съобрази с всички забележки, направени от надзорния орган по отношение на обработката на изпратените данни.

Ако Субект на данни твърди, че настоящата Политика за защита на данните е била нарушена от дружество от Ipsos Group, намиращо се в друга държава, което получава данните, дружеството от Ipsos Group, което изпраща Личните данни, се ангажира да подкрепи въпросния Субект на данни за установяване на фактите по случая, и също така за да защити своите права в съответствие с настоящата Политика за защита на данните срещу дружеството от Ipsos Group, което получава данните. Освен това, Субектите на данни имат право да предявят своите права срещу дружеството от Ipsos Group, което

изпраща данните. В случай на претенции за нарушение, дружеството изпращач трябва да подкрепи с факти пред Субектите на данни, че дружеството, получаващо Личните данни, не е нарушило настоящата Политика за защита на данните.

Всяко дружество от Ipsos Group, изпращащо Лични данни на дружество от Ipsos Group, намиращо се в друга държава, остава отговорно за всяко нарушение на настоящата Политика за защита на данните, извършено от дружеството от Ipsos Group, получило Личните данни, все едно че нарушението е извършено от компанията от Ipsos Group, изпращаща Личните данни.

Всяко изпращане на Лични данни в рамките на Ipsos Group се извършва само след като е направено съответното вписване в JobBook за проекта, по който е направено изпращането. Това вписване създава договор съгласно Основното вътрешногрупово споразумение за услуги на Ipsos и автоматично направи съответните стандартни клаузи на ЕС приложими към това изпращане.

7. Обработка на данни от външни доставчици/трети страни

В много случаи Ipsos използва външни доставчици за обработката на Лични данни. В тези случаи със съответния доставчик трябва да бъде сключено споразумение за обработка на данни от името на Ipsos. Това може да стане или чрез включване на съответните разпоредби в споразумението, уреждащо цялостните отношения с доставчика, или в отделен конкретен документ. По отношение на обработката от името на Ipsos, доставчикът може да обработва Лични данни само съгласно инструкциите на Ipsos. Когато се дават инструкции на доставчик, трябва да бъдат спазени следните изисквания:

- Когато въпросните Лични данни попадат в параграф 5.2 (клиентски данни), всички релевантни изисквания на клиента трябва да бъдат предадени на доставчика.
- Доставчикът трябва да бъде избран въз основа на неговата способност да покрие необходимите технически и организационни защитни мерки и в съответствие с процеса на одобрение на доставчици на Ipsos.
- Доставчикът не трябва да наема подизпълнители за обработката без предварителното писмено съгласие на Ipsos.
- Инструкциите трябва да бъдат изпратени в писмен вид чрез съответния договор. Инструкциите за обработка на данни и отговорностите на Ipsos и доставчика трябва да бъдат документирани.
- Преди да започне обработката на данните, Ipsos трябва да е уверена, че доставчикът ще изпълни задълженията си. Доставчикът може да документира спазването на изискванията за сигурност на данните, по-специално като представи съответния сертификат. В зависимост от риска при обработката на данните, проверките трябва да се повтарят редовно през срока на валидност на договора. Ipsos си запазва правото да одитира съответствието на доставчика.
- В случай на трансгранична обработка на данни по договор, трябва да бъдат спазени съответните национални изисквания за разкриване на Лични данни в чужбина. По-специално, Лични данни от Европейското икономическо пространство могат да се обработват в трета държава само ако доставчикът може да докаже, че има стандарт за защита на данните, еквивалентен на GDPR и настоящата Политика за защита на данните. Подходящи инструменти могат да бъдат:
    - споразумение, базирано на стандартни договорни клаузи на ЕС за обработване на данни в трети страни по договор с доставчика. Подобни споразумения ще се изискват за всеки подизпълнител на доставчика.

- участие на доставчика в сертификационна система, акредитирана от ЕС за предоставяне на достатъчно ниво на защита на данните.

8. Права на Субекта на данни

Всеки Субект на данни има следните права. Искането им се обработва незабавно от съответната компания на Ipsos и не може да води до каквито и да било неблагоприятни последици за Субекта на данни. Когато съответните Лични данни се обработват от Ipsos съгласно параграф 5.2 Лични данни, предоставени от клиенти, трябва да се направи преглед на съответният договор с клиента по отношение на всеки процес, който трябва да бъде следван и клиентът трябва незабавно да бъде информиран за такова искане.

- **Право на достъп:**
  - Субектите на данни могат да поискат информация за това какви свързани с тях Лични данни се съхраняват, как са събрани данните и за каква цел.
  - Ако Личните данни се предават на трети страни, трябва да се предостави информация за самоличността на получателя или за категориите получатели, включително и за други компании от Ipsos.
- **Право на поправка:** Ако Личните данни са неправилни или непълни, Субектът на данни може да поиска тяхното коригиране или допълване.
- **Право на отказ от съгласие:** Когато Личните данни се обработват въз основа на Съгласие (виж също отделните указания относно Съгласието), Субектите на данни могат по всяко време да възразят срещу обработката им. Тези Лични данни трябва да бъдат блокирани от обработката, срещу която са били повдигнати възражения.
- **Право за изтриване.** Субектът на данни може да поиска данните му да бъдат изтрити, ако обработването на тези данни няма правно основание или ако правното основание вече не се прилага. Същото важи и ако целта за обработката на данни вече не съществува или вече не е приложима по други причини. Трябва да се спазват съществуващите периоди на съхраняване и противоречието на интереси, които заслужават защита.
- **Право на възражение:** Субектите по данни като цяло имат право да възразят срещу обработването на техните данни и това трябва да бъде взето предвид, ако защитата на техните интереси има предимство пред интересите на администратора на данни поради конкретната лична ситуация. Това не се прилага, ако правна разпоредба изисква Личните данни да бъдат обработвани.
- **Право на преносимост на данни.** Субектът на данни има право да поиска предоставените от него Лични данни да бъдат на негово разположение в лесно четим формат, като например Word или Excel документ.

9. Поверителност на обработката

Личните данни са тайна. Всяко неразрешено събиране, обработка или използване на такива данни от служители е забранено. Всяко обработване на данни от страна на служител, за което той не е бил оторизиран да прави като част от неговите законни задължения, е неоторизирано. Прилага се принципът "необходимост да се знае". Служителите могат да имат достъп до Лични данни само според както е подходящо за вида и обхвата на конкретната задача. Това изисква внимателна разбивка и разделяне, както и ограничаване на ролите и отговорностите. Освен това се прилагат изискванията на Политиката за управление на информацията.

На служителите е забранено да използват Лични данни за свои лични или търговски цели, да ги разкриват на неупълномощени лица или да ги предоставят по какъвто и да е друг начин. Ръководителите трябва да информират служителите в началото на трудовото правоотношение относно задължението за запазване на тайната на данните. Това задължение остава в сила дори след приключване на трудовите правоотношения. Трудовите договори с персонала на Ipsos трябва да съдържат съответните задължения за поверителност.

10. Поверителност на етапа на проектирането и по подразбиране

Ipsos ще използва подхода на "Поверителност на етапа на проектирането и по подразбиране" (*Privacy by Design and by Default*) в цялата си работа, но по-специално когато:

- изгражда нови ИТ системи за съхранение на или достъп до Лични данни;
- разработва нови приложения или изследователски подходи;
- започва инициатива за обмен на данни; или
- използва данни за нови цели.

Поверителност на етапа на проектирането е проектен подход, който насърчава спазването на поверителността и защитата на данните от самото начало. Това е ключово съображение в ранните етапи на всеки проект, а след това и през целия му жизнен цикъл.

Приемането на подход за поверителност на етапа на проектирането е основен инструмент за минимизиране на рисковете за поверителността и за изграждане на доверие, и ще спомогне за планирането на проекти, процеси, продукти или системи, които вземат предвид поверителността още от самото начало.

По отношение на дадените по-горе примери, необходимият инструмент за съответствие е изготвянето на Оценка на въздействието върху защитата на данните.

11. Сигурност на обработката

Личните данни трябва да бъдат защитени от неразрешен достъп или разкриване (без значение дали вътре или извън организацията), незаконна обработка, както и случайна загуба, промяна или унищожаване. Това важи независимо дали данните се обработват по електронен път или на хартиен носител. Освен защитата на съществуващите Лични данни в съответствие с приложимите политики на Ipsos (моля, вижте глава 7 от Книга на политиките и процедурите на Ipsos, която е приложима в това отношение), преди въвеждането на нови методи за обработка на данни, конкретни нови информационни системи или изследователски подходи, трябва да бъдат определени и въведени технически или организационни мерки за защита на Личните данни. Тези мерки трябва да са базирани на състоянието на техниката, риска от обработка и необходимостта от защита на данните.

Тези технически и организационни мерки трябва да бъдат договорени след консултация със съответния Служител по сигурността на информацията и Служител по защита на данните (DPO). Техническите и организационни мерки за защита на Личните данни са част от управлението на Корпоративната информационна сигурност и трябва непрекъснато да

се адаптират към техническото развитие и напредъка, както и към организационните промени.

Като минимум, Ipsos ще обработва всички Лични данни, които притежава, в съответствие със своята Политика за сигурност, и ще взема подходящи мерки за сигурност срещу незаконна или неразрешена обработка на Лични данни и срещу случайна загуба или повреда на Лични данни.

12. Одит на защитата на данните

Спазването на настоящата Политика за защита на данните и на приложимите закони за защита на данните се проверява редовно с одити на защитата на данните и с други контроли. Изпълнението на тези контроли е отговорност на Главния служител по защита на личната информация (CPO), Служителя по защита на данните (DPO), Вътрешния одит и/или външни наети одитори. Различните клиенти на Ipsos също имат право на одит съгласно техните споразумения с Ipsos. Резултатите от одитите на защитата на данните трябва да бъдат докладвани на Главния служител по защита на личната информация (CPO) и на Началника по съответствието. При поискване резултатите от одитите на защитата на данните ще бъдат предоставени на компетентните органи по защита на данните.

13. Инциденти, свързани със защитата на данните

Всички служители трябва незабавно да информират своя Служител по защита на данните (DPO) или Главния служител по защита на личната информация (CPO) за случаи на нарушения на настоящата Политика за защита на данните или на други разпоредби за защита на Личните данни, в съответствие с Процедурата за управление на нарушенията на личните данни, която също може да бъде намерена в раздел 8 от Книга на политиките и процедурите на Ipsos. Всеки пропуск да се обърне внимание на сериозните недостатъци, свързани с тази Политика, може да бъде докладван и по системата "Ipsos Whistle-blowing".

В случай на:

- неправомерно изпращане на Лични данни на трети страни;
- неправомерно изпращане на Лични данни през граница;
- неправомерен достъп до Лични данни, включително от трети лица, или
- загуба на Лични данни (включително които след това са станали публични поради вътрешни нередности),

трябва незабавно да бъде направено уведомление за нарушение на защитата на данните, за да се гарантира, че а) могат да бъдат спазени всички задължения за докладване съгласно националното законодателство, б) всеки засегнат клиент може да бъде информиран и в) всяка комуникация със заинтересованите страни може да бъде управлявана. Всяко нарушение на Защитата на данните представлява и инцидент по сигурността на информацията в рамките на Политиката за управление на инцидентите в областта на информационните технологии.

14. Отговорности и санкции

14.1. Управление

Изпълнителните органи на съответните компании от Ipsos Group отговарят за обработката на данните в своята област на отговорност. Поради тази причина, от тях се изисква да гарантират, че законовите изисквания за защита на данните, както и тези, съдържащи се в настоящата Политика за защита на данните (например националните задължения за докладване), са изпълнени.

Ръководството отговаря за осигуряването на организационни, човешки ресурси и технически мерки, така че всяка обработка на данни да се извършва в съответствие с тези изисквания за защита на данните.

Съответствието с тези изисквания е отговорност и на съответните служители.

Ако официални агенции правят одити на защитата на данните, Главният служител по защита на личната информация (CPO) трябва да бъде информиран незабавно.

Съответните ръководители по държави в Ipsos трябва да информират Главния служител по защита на личната информация (CPO) за името на Служителя по защита на данните (DPO).

Неправилната обработка на Лични данни или други нарушения на законите за защита на данните могат да бъдат обект на наказателно преследване в много страни и да доведат до искове за обезщетение за вреди. Освен това, нарушенията, за които са отговорни отделни служители, могат да доведат до санкции по трудовото законодателство.

14.2. Служители по защита на данните (DPOs)

Всяка държава, в която работи Ipsos, трябва да назначи един или повече Служители по защита на данните (**DPO**). Служителите по защита на данните (DPO) са вътрешните и външни лица за контакт в дадената държава във връзка със защитата на данните. Те могат да извършват проверки и трябва да запознаят служителите със съдържанието на настоящата Политика за защита на данните и с приложимото законодателство. Съответните ръководители са длъжни да помагат на Служителите по защита на данните (DPO) в тяхната работа. Основните задачи на всеки Служител по защита на данните (DPO) са:

- *Да информира и консултира организацията и нейните служители за техните задължения да спазват приложимите закони за защита на данните и настоящата Политика за защита на данните.* Тази задача ще бъде подкрепяна и ръководена от Групата и чрез мрежата от Служители по защита на данните (DPOs) под ръководството на Главния служител по защита на личната информация (CPO) и чрез обучение.
- *Да следи за спазването на законите за защита на данните, включително управлението на вътрешните дейности за защита на данните, да съветва относно (но не и да провежда) оценките на въздействието върху защитата на данните; да обучава персонала и да провежда вътрешни одити.* Това ще бъде подкрепяно и ръководено от Групата. Одитите, различни от проверките на място, трябва да бъдат координирани с отдела по вътрешен одит на Групата.

- *Да бъде първата точка за контакт за надзорните органи и за лицата, чиито данни се обработват (служители, клиенти и т.н.).*

В рамките на всяка държава, в която работи Ipsos, Служителят по защита на данните (DPO) ще трябва:

- Да докладва на най-високото ниво на управление на организацията в страната, в която работи Ipsos, т.е. на ниво местен управителен съвет или член.
- Да работи независимо от професионалните поръчки, и не се освобождава или наказва за изпълнение на задачата си.
- Да разполага с необходимите ресурси, за да може Служителят по защита на данните (DPO) да изпълнява задълженията си съгласно приложимите закони за защита на данните и настоящата Политика за защита на данните.

Служителите по защита на данните незабавно информират Главния служител по защита на личната информация (CPO) за всички рискове, свързани със защитата на данните.

14.3. Главен служител по защита на личната информация на глобално ниво

Главният служител по защита на личната информация (**CPO**) на глобално ниво, който е вътрешно независим от професионалните поръчки, работи за спазването на националните и международните разпоредби за защита на данните. Той/тя отговаря за настоящата Политика за защита на данните и извършва надзор върху спазването ѝ.

Всеки Субект на данни може по всяко време да се обърне към Главния служител по защита на личната информация (CPO) или към съответния Служител по защита на данните (DPO), за да изрази притеснения, да зададе въпроси, да поиска информация или да подаде оплаквания, свързани с въпроси, касаещи защитата на данните или сигурността на данните. При поискване, опасенията и жалбите ще бъдат третирани поверително.

Ако съответният Служител по защита на данните (DPO) не може реши жалба или да отстрани нарушение на Политиката за защита на данните, той трябва незабавно да се консултира с Главния служител по защита на личната информация (CPO). Решенията на CPO за отстраняване на нарушенията на защитата на данните трябва да бъдат потвърдени от ръководството на съответното дружество. Запитванията от надзорните органи трябва винаги да се докладват на CPO.

15. Дерогация

В изключителни случаи може да е възможно да се получи дерогация от настоящата Политика, преди всяка планирана обработка на засегнатите Лични данни. Всяка такава дерогация може да бъде предоставена само след пълна оценка на въздействието върху защитата на данните, за да се установят и оценят рисковете за засегнатия Субект на данни, правните рискове и въздействието върху репутацията, и това подлежи на одобрение от страна на отдела, подпомагащ Президента на Ipsos.

16. Речник

Администратор на данни/Администратор/Съвместен администратор

Това е лицето или организацията, която определя целите и начина, по който се обработват Личните данни. Той отговаря за установяването на практики и политики в съответствие с приложимите законови изисквания.

В повечето случаи, когато Ipsos получава извадка от клиент, той става съвместен администратор на събраните данни. Това обхваща данните, които събираме, дори когато сме уверили респондентите в поверителността на техните отговори. Отговорностите и задълженията на съвместните администратори трябва да бъдат документирани и изяснени в писмено споразумение.

Някои юрисдикции използват други изрази за същата концепция като например **Отговорно лице, Организация, Оператор**[1] и др.

Потребители на данни

Това са онези от нашите служители, чиято работа включва обработката на Лични данни. Потребителите на данни трябва по всяко време да защитават данните и Личните данни, които обработват, в съответствие с настоящата Политика и с всички приложими процедури за сигурност на данните.

Обработващ данни или Обработчик

Това е лице или организация, които не са Потребител на данни, и които обработват Лични данни от името и по нареждане на Администратора. Служителите на администраторите на данни са изключени от това определение, но то може да включва доставчици, които обработват Лични данни. Ipsos може понякога да бъде Администратор (например по отношение на участниците в наши групи или в ad-hoc извадки, които Ipsos наема за дадено проучване) или Обработващ данните (например по отношение на извадка, предоставена от клиенти). Някои юрисдикции използват други изрази за същата концепция, като например **Трета страна, Посредник, Оператор**[2] и др.

Субекти на данни

За целите на настоящата Политика това са всички реални лица, по отношение на които фирмата Ipsos притежава Лични данни. Не е задължително Субектът на данни да бъде гражданин или пребиваващ в страната. Всички Субекти на данни имат законни права във връзка с тяхната лична информация.

Лични данни

Дефиницията за Лични данни от GDPR (член 4, алинея 1 от GDPR) изразява ясно какво означават Личните данни и показва, че те трябва да се интерпретират широко:

[1] Сингапур

[2] Южна Африка

"... всяка информация, свързана с идентифицирано физическо лице или физическо лице, което може да бъде идентифицирано („субект на данни“); физическо лице, което може да бъде идентифицирано, е лице, което може да бъде идентифицирано, пряко или непряко, по-специално чрез идентификатор като име, идентификационен номер, данни за местонахождение, онлайн идентификатор или по един или повече признаци, специфични за физическата, физиологичната, генетичната, психическата, умствената, икономическата, културната или социална идентичност на това физическо лице ".

Всяко физическо лице е реален индивид, а самият GDPR не се прилага за починали лица. Въпреки това, отделните държави-членки могат да предвидят правила относно обработката на Лични данни дори по отношение на починали лица.

Фирмената информация не представлява Лични данни.

Трябва да се признае, че не винаги е възможно да се определи с абсолютна сигурност дали отделна информация би представлявала Лични данни. Ще бъде необходимо да се разгледа цялостната информация, която се притежава за въпросното лице или средствата, които е разумно вероятно да се използват, за да се идентифицира даден човек. С все по-усъвършенстваните технологични средства, все повече данни ще стават Лични данни.

Обработване

Обработването е всяка дейност, която включва използване на данните. Това включва получаване, записване или съхраняване на данните или извършване на всяка операция или набор от операции върху данните, включително организиране, изменение, извличане, използване, разкриване, изтриване или унищожаване на данните. Обработването включва и изпращането на Лични данни.

Специални категории данни (p/k/a лични чувствителни данни)

"Специални категории данни" е новият израз, използван в GDPR, който преди се наричаше "чувствителни данни". Понастоящем те са определени в член 9 от GDPR като данни относно:

расов или етнически произход, политически възгледи, религиозни или философски убеждения или членство в синдикални организации, генетични данни [виж по-долу], биометрични данни [виж по-долу] с цел еднозначно идентифициране на дадено физическо лице, данни за здравословното състояние [виж по-долу] или данни за сексуалния живот или сексуалната ориентация на физическото лице.

За някои от тези изрази в GDPR са дадени по-подробни определения:

„генетични данни“ означава Лични данни, свързани с наследени или придобити генетични характеристики на дадено физическо лице, които дават уникална информация за физиологията или здравето на това физическо лице, и които са получени, по-специално, от анализ на биологична проба от въпросното физическо лице;

„биометрични данни“ означава Лични данни, получени в резултат на специфично техническо обработване, които са свързани с физическите, физиологичните или поведенческите характеристики на дадено физическо лице, и които позволяват или

потвърждават уникалната идентификация на това физическо лице, като лицеви изображения или дактилоскопични данни;

„данни за здравословното състояние“ означава Лични данни, свързани с физическото или психичното здраве на дадено физическо лице, включително предоставянето на здравни услуги, които дават информация за здравословното му състояние;

Анонимни данни

Това се определя като информация, която не е свързана с идентифицирано или подлежащо на идентификация физическо лице или с Лични данни, които са анонимни по такъв начин, че Субектът на данни не е или вече не може да бъде идентифициран (GDPR съображение (26)). Те трябва да се различават от данните, които, заедно с използването на допълнителна информация (например ключ), могат да бъдат използвани за идентифициране на дадено физическо лице, след което данните са само псевдонимизирани.

Псевдонимизираните данни все пак попадат в обхвата на определението за Лични данни и все пак ще се прилагат пълните принципи и изисквания на GDPR.

Псевдонимизация

Псевдонимизация означава обработването на Лични данни по такъв начин, че Личните данни вече да не могат да бъдат приписани на конкретен Субект на данни без използването на допълнителна информация, при условие че тази допълнителна информация се съхранява отделно и подлежи на технически и организационни мерки, за да се гарантира че Личните данни не се приписват на идентифицирано или подлежащо на идентификация физическо лице. (член 4, алинея 5 от GDPR).

Псевдонимизирани данни се отнасят до данни, в които идентификаторите в даден набор от данни се заменят с изкуствени идентификатори или псевдоними, които се съхраняват отделно и подлежат на технически защитни мерки. Псевдонимизираните данни остават Лични данни и следователно по отношение на тях продължават да се прилагат всички останали изисквания за защита на данните!!

PII или Лично разпознаваема информация

Този термин произхожда от американското законодателство за защита на личната информация. Въпреки че от практическа гледна точка, приложима към ежедневната работа на Ipsos, изразите Лични данни и Лично разпознаваема информация могат да се разглеждат като синоними, използването на израза Лично разпознаваема информация в контекста на GDPR трябва да се избягва, тъй като в противен случай това ще има отрицателно въздействие върху нашето задължение да доказваме съответствие. Регулаторите имат голям интерес към последователността и точността при използването на изразите.

PHI или Защитена здравна информация

Този термин също произлиза от американското законодателство за защита на личната информация, и по-специално от Закона за преносимостта и отчетността на здравното осигуряване (HIPPA). Въпреки че от практическа гледна точка, приложима към ежедневната работа на Ipsos, изразите Лични данни и Лично разпознаваема информация трябва да се разглеждат като синоними, използването на израза Лично разпознаваема информация в контекста на GDPR трябва да се избягва.

Основният въпрос, който трябва да се разглежда тук е, че определени Лични данни, които попадат в обхвата на правната дефиниция за Защитена здравна информация, съгласно GDPR представляват Лични данни, а не специални категории данни. Например, HIPPA разглежда цялата информация в даден списък с данни, която съдържа име и сексуална ориентация като Защитена здравна информация, докато GDPR счита само сексуалната ориентация като част от специалните категории Лични данни.

PSI или Лична чувствителна информация

Този израз вече е остарял, тъй като произтича от предходното законодателство. Той до голяма степен е синоним на "специални категории Лични данни", съгласно определението в член 9 от GDPR, и трябва да се използва този израз. Регулаторите ще очакват Ipsos да използва правилната терминология, за да демонстрираме нашето съответствие като част от задължението ни за отчетност.

Контрол върху документа (член 25 от GDPR)

Версия	**Дата**	**Обобщение на промените**	**Автори**	**Одобрен от**
1.0	12.04.2018 г.	Версия, одобрена за публикуване	Рупърт ван Хулен	**Лорънс Стоклет**

Преглед на документа	
Дата на последен преглед	12.04.2018 г.
Версия, обект на прегледа	1.0
Предложени промени (списък на номера на раздела и кратко описание на промените)	N/A
Комисия по прегледа	CPO, GC, CIO, MarCom
Одобряващ орган/ Комитет	Заместник Главен изпълнителен директор и Главен финансов директор
Дата на следващ преглед	12.04.2019 г.
Забележка: Записите в тази таблица не водят до промяна в номера на версията.	