СТАНДАРТИЗИРОВАННАЯ ПОЛИТИКА БЕЗОПАСНОСТИ

Настоящая стандартизированная политика безопасности (далее – Политика безопасности) действует в отношении всех персональных данных, полученных от субъекта персональных данных (далее по тексту – «Пользователя») или его представителя, которую саит в информационно-телекоммуникационнои сети Интернет, расположенныи на доменном имени starlinedesign.ru (далее по тексту – «Саит»), принадлежащии студии графического дизайна Starline (далее по тексту – «Оператор»), может получить о Пользователе во время использования Саита, его программ и продуктов.

1. При обработке персональных данных Пользователя Оператор принимает необходимые правовые, организационные и технические меры, необходимые и достаточные для обеспечения выполнения обязанностей, предусмотренных Федеральным законом РФ № 152-ФЗ от 27.07.2006 «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, а также для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения персональных данных, а также от иных неправомерных действий в отношении персональных данных.
2. К таким мерам, в частности, относятся:

1) изданием настоящей Политики безопасности и опубликованием ее информационно-телекоммуникационной сети Интернет на своем Сайте;
2) доведением до неопределенного круга лиц информации об Операторе, содержащей его наименование, основной государственный регистрационный номер налогоплательщика, идентификационный номер налогоплательщика, место нахождения (адрес), адрес электронной почты;
3) установлением стандартизированного Согласия на обработку персональных данным физическим лицом;
4) назначение Оператором, являющимся юридическим лицом, ответственного за организацию обработки персональных данных;
5) ознакомление работников Оператора, непосредственно осуществляющих обработку персональных данных, с положениями законодательства Российской Федерации о персональных данных, в том числе требованиями к защите персональных данных, установленных локальными документами Оператора;
6) установлением типовой формы согласия работников Оператора на обработку персональных данных;
7) установлением типового обязательства работника Оператора, осуществляющего обработку персональных данных, в случае расторжения с ним трудового договора прекратить обработку персональных данных, ставших известными ему в связи с исполнением трудовых обязанностей;
8) организацией обучения работников Оператора, обрабатывающих персональные данные;
9) установлением правил обработки персональных данных, устанавливающих процедуры, направленные на выявление и предотвращение нарушений законодательства РФ в сфере персональных данных, а также определяющих для каждой цели обработки персональных данных содержание обрабатываемых персональных данных, категории Пользователей, персональные данные которых обрабатываются, сроки их обработки и хранения, порядок уничтожения при достижении целей обработки или при наступлении иных законных оснований;
10) установлением правил рассмотрения запросов Пользователя или его представителя;
11) установлением правил осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных, установленным федеральными законами, принятыми в соответствии с ним нормативными правовыми актами и локальными актами Оператора;
12) установлением правил работы с обезличенными данными в случае обезличивания персональных данных;
13) установлением правил доступа к персональным данным, обрабатываемым в информационной системе персональных данных, а также обеспечением регистрации и учета всех действий, совершаемых с персональными данными в информационной системе персональных данных;

14) определением перечней информационных систем персональных данных;
15) определением перечня персональных данных, обрабатываемых Оператором;
16) установлением должностных обязанностей или должностных инструкций лица, ответственного за организацию обработки персональных данных, и работников Оператора, осуществляющих обработку персональных данных;
17) установлением порядка доступа работников Оператора в помещения, в которых ведется обработка персональных данных;
18) установлением организационных и технических мер по обеспечению безопасности персональных данных при их обработке;
19) определением угроз безопасности персональных данных при их обработке в информационных системах персональных данных;
20) применением прошедших в установленном порядке процедуру оценки соответствия средств защиты информации;
21) оценкой эффективности принимаемых мер по обеспечению безопасности персональных данных до ввода в эксплуатацию информационной системы персональных данных;
22) оценкой вреда, который может быть причинен Пользователю в случае нарушения требований в области защиты персональных данных;
23) учетом машинных носителей персональных данных;
24) проверками и обеспечением технической укрепленности помещений, в которых обрабатываются персональные данные, хранится относящаяся к их обработке документация;
25) обнаружением фактов несанкционированного доступа к персональным данным и принятием мер;
26) сообщением в правоохранительные органы о фактах несанкционированного доступа к персональным данным;
27) восстановлением персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;
28) проведением периодических проверок условий обработки персональных данных ответственным за организацию обработки персональных данных лицом либо комиссией, образуемой Оператором;
29) осуществлением внутреннего контроля и (или) аудита соответствия обработки персональных данных федеральным законам и принятым в соответствии с ними нормативными правовыми актами, требованиям к защите персональных данных, Политике безопасности Оператора в отношении обработки персональных данных, локальным актам Оператора;
30) уведомлением уполномоченного органа по защите прав субъектов персональных данных об обработке (намерении осуществлять обработку) персональных данных, за исключением случаев, установленных федеральными законами;
31) представлением документов и локальных актов Оператора и (или) иным образом подтверждением принятие мер по защите персональных данных уполномоченному органу по защите прав субъектов персональных данных.