Утверждена
приказом Исполнительного директора
НПФ «Волга-Капитал»
№ 66/1 от 27 апреля 2011г.

# ПОЛИТИКА
# НПФ «Волга-Капитал»
# в отношении обработки персональных данных

Казань, 2011

## 1. Общие положения

1.1. Настоящее положение определяет политику НПФ «Волга-Капитал» (далее – Фонд) в отношении обработки персональных данных и содержит сведения о реализуемых требованиях к защите персональных данных.

1.2. Политика Фонда в отношении обработки персональных данных осуществляется в соответствии с требованиями законодательства РФ и основана на следующих принципах:

1.2.1. Обработка персональных данных должна осуществляться на законной и справедливой основе.

1.2.2. Не допускается обработка персональных данных, несовместимых с целями сбора персональных данных.

1.2.3. Содержание и объем обрабатываемых персональных данных должны соответствовать заявленным целям обработки.

1.2.4. При обработке персональных данных должна быть обеспечена точность персональных данных, их достаточность и актуальность по отношению к целям обработки персональных данных.

1.2.5. По достижении целей обработки или в случае утраты необходимости в достижении этих целей, персональные данные должны быть уничтожены или обезличены, если иное не предусмотрено федеральным законом.

1.3. Обработка персональных данных в Фонде осуществляется в следующих случаях:

- с согласия субъекта персональных данных на обработку его персональных данных;
- обработка персональных данных необходима для достижения целей, предусмотренных законом, для осуществления и выполнения возложенных законодательством Российской Федерации на оператора функций, полномочий и обязанностей;
- обработка персональных данных необходима для исполнения договора, стороной которого либо выгодоприобретателем или поручителем по которому является субъект персональных данных, а также для заключения договора по инициативе субъекта персональных данных или договора, по которому субъект персональных данных будет являться выгодоприобретателем или поручителем;
- обработка персональных данных необходима для осуществления прав и законных интересов оператора или третьих лиц либо для достижения общественно значимых целей при условии, что при этом не нарушаются права и свободы субъекта персональных данных;
- осуществляется обработка персональных данных, доступ неограниченного круга лиц к которым предоставлен субъектом персональных данных либо по его просьбе (далее - персональные данные, сделанные общедоступными субъектом персональных данных);
- осуществляется обработка персональных данных, подлежащих опубликованию или обязательному раскрытию в соответствии с федеральным законом.

## II. Соблюдение требований по защите персональных данных

2.1. С целью обеспечения безопасности персональных данных при их обработке в Фонде реализуются требования следующих нормативных документов РФ в области обработки и обеспечения безопасности персональных данных:

- Федеральный закон от 27.07.2006 г. № 152-ФЗ «О персональных данных»;
- постановление Правительства Российской Федерации от 17.11.2007 г. № 781 «Об утверждении Положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных»;

- постановление Правительства Российской Федерации от 15.09.2008 г. № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»;

- порядок проведения классификации информационных систем персональных данных (утвержден приказом ФСТЭК России, ФСБ России и Мининформсвязи России от 13.02.2008 г. № 55/86/20);

- базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных (утверждена заместителем директора ФСТЭК России 15.02.2008 г.);

- методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных (утверждена заместителем директора ФСТЭК России 14.02.2008 г.);

- типовые требования по организации и обеспечению функционирования шифровальных (криптографических) средств, предназначенных для защиты информации, не содержащей сведений, составляющих государственную тайну в случае их использования для обеспечения безопасности персональных данных при их обработке в информационных системах персональных данных (утверждены руководством 8 центра ФСБ России 21.02.2008 г. № 149/6/6-622);

- методические рекомендации по обеспечению с помощью криптосредств безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств автоматизации» (утверждены руководством 8 Центра ФСБ России 21.02.2008 г. №149/5-144);

- положение о методах и способах защиты информации в информационных системах персональных данных (утверждено приказом ФСТЭК России от 05.02.2010 г. № 58;

- отраслевые стандарты обеспечения безопасности персональных данных (НАПФ).

2.2. Меры, направленные на обеспечение выполнения Фондом обязанностей, по защите персональных данных:

- назначение Фондом, ответственного лица за организацию обработки персональных данных;

- разработка Фондом необходимой организационно – распорядительной документации по вопросам обработки персональных данных;

- применение правовых, организационных и технических мер по обеспечению безопасности персональных данных;

- осуществление внутреннего контроля и (или) аудита соответствия обработки персональных данных действующему законодательству и принятым в соответствии с ним нормативным правовым актам, требованиям к защите персональных данных, локальным актам Фонда.

2.3. Обеспечение безопасности персональных данных достигается, в частности:

- определением угроз безопасности персональных данных при их обработке в информационных системах персональных данных;

- применением организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, необходимых для выполнения требований к защите персональных данных;

- применением прошедших в установленном порядке процедуру оценки соответствия средств защиты информации;

- оценкой эффективности принимаемых мер по обеспечению безопасности персональных данных до ввода в эксплуатацию информационной системы персональных данных;

- учетом машинных носителей персональных данных;

- обнаружением фактов несанкционированного доступа к персональным данным и принятием мер;

- восстановлением персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;

- 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;

- контролем за принимаемыми мерами по обеспечению безопасности персональных данных и уровня защищенности информационных систем персональных данных.