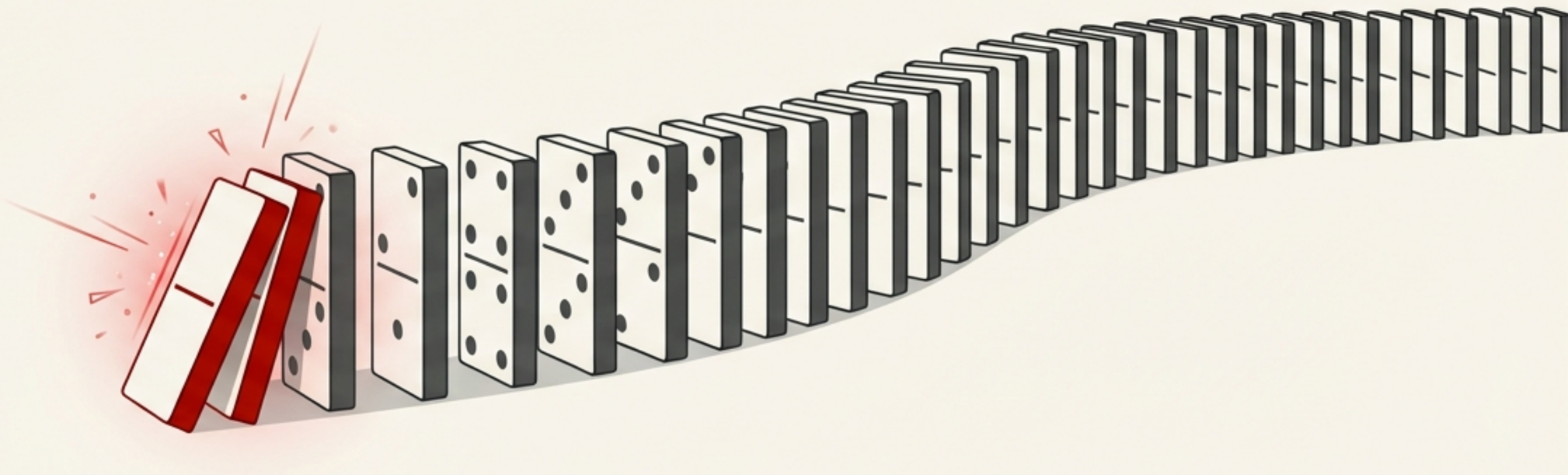
보이지 않는 지뢰: 크롤링 전화번호를 이용한 선거 문자의 법적 위험

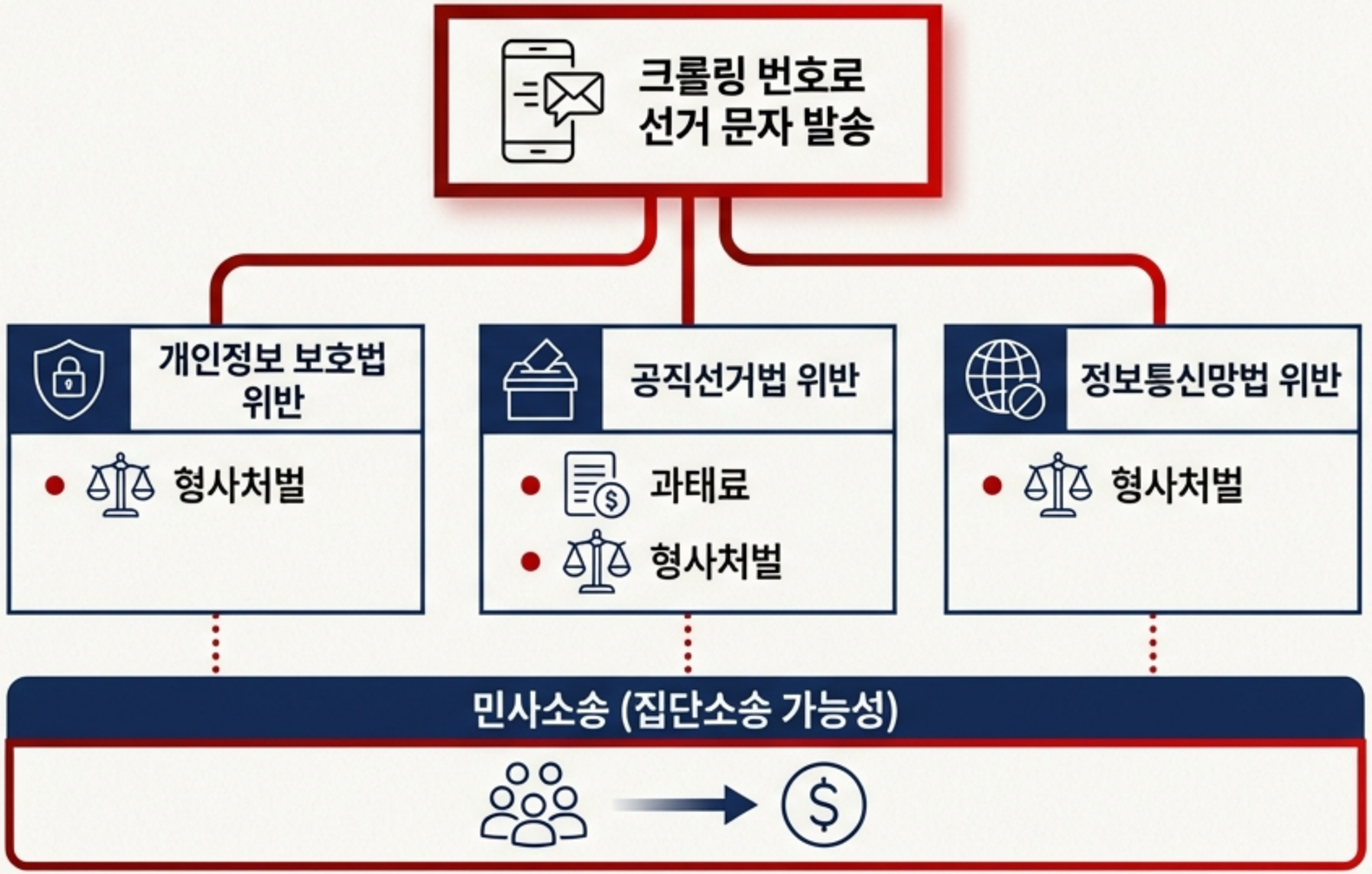
단 한 번의 잘못된 전송이 선거 캠페인 전체를 무너뜨리는 이유



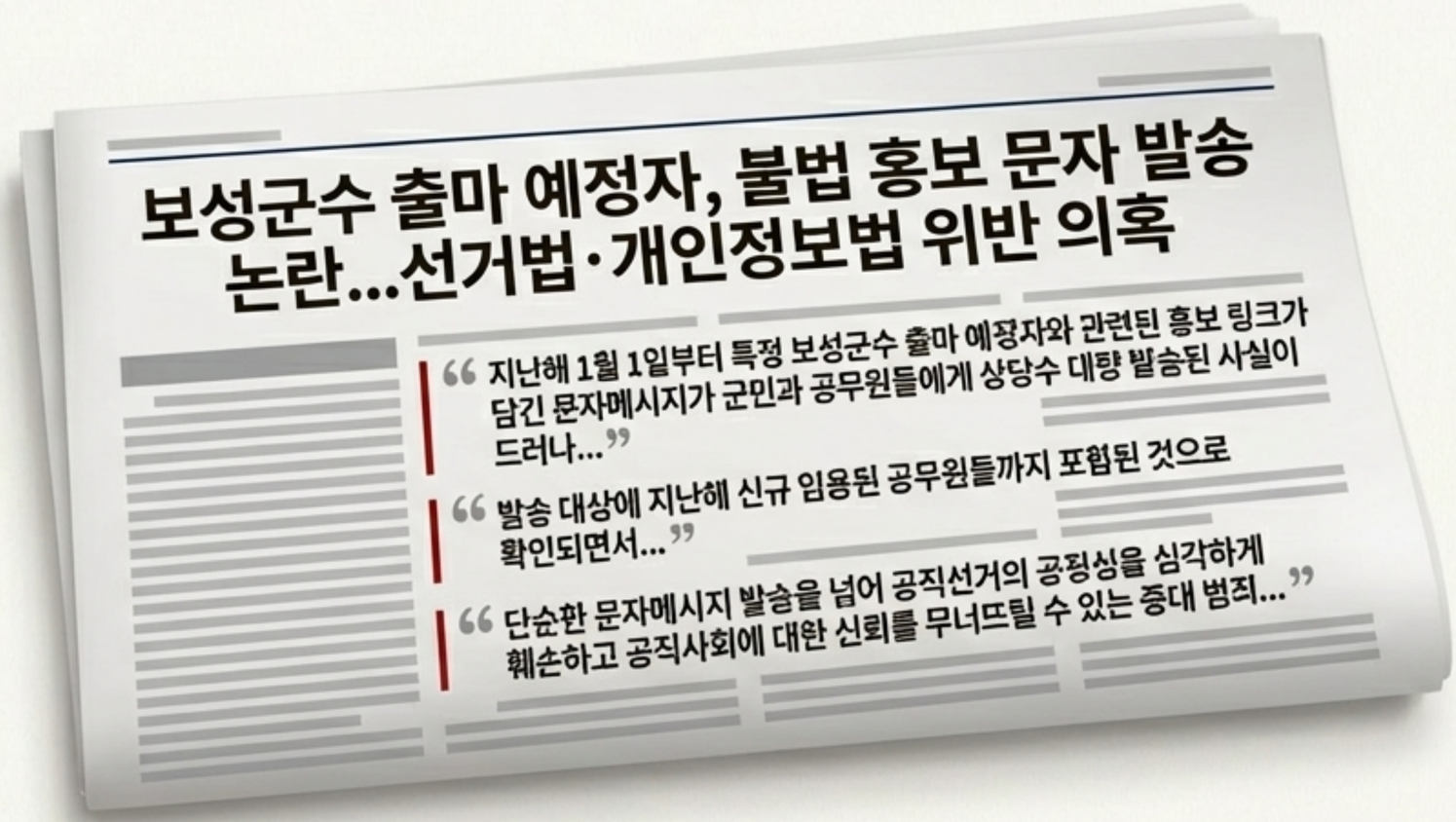
하나의 행위, 세 개의 법률 위반: '책임 중첩(Stacked Liability)'의 구조

핵심 개념 (Core Concept)

인터넷에서 크롤링한 휴대폰 번호로 선거 문자를 보내는 행위는 단순 과태료 사안이 아닙니다.
이 행위는 개인정보 보호법, 공직선거법, 정보통신망법을 동시에 위반하여, 각 법률에 따른 형사, 행정, 민사 책임을 중첩적으로 발생시킵니다.



이 위험은 이론이 아닌 현실입니다: 보성군수 출마 예정자 사례



보성군수 출마 예정자, 불법 홍보 문자 발송 논란…선거법·개인정보법 위반 의혹

“지난해 1월 1일부터 특정 보성군수 출마 예정자와 관련된 홍보 링크가 담긴 문자메시지가 군민과 공무원들에게 상당수 대량 발송된 사실이 드러나…”

“발송 대상에 지난해 신규 임용된 공무원들까지 포함된 것으로 확인되면서…”

“단순한 문자메시지 발송을 넘어 공직선거의 공정성을 심각하게 훼손하고 공직사회에 대한 신뢰를 무너뜨릴 수 있는 중대 범죄…”

보성군 사례는 데이터의 출처가 불분명할 경우, 사전선거운동, 공무원 중립의무 위반, 개인정보보호법 위반 등 복합적인 법적 문제로 비화됨을 명확히 보여줍니다. 이는 모든 캠페인이 직면할 수 있는 실제 리스크입니다.

제1단계 위법: 모든 문제의 시작, '불법 데이터 수집'

인터넷에 공개된 정보 ≠ 사용에 동의한 정보

허용된 목적 (Permitted Purpose)

목적 외 불법 사용 (Illegal External Use)

- 개인정보 보호법(PIPA)의 핵심은 '정보주체의 동의'입니다.
- 웹사이트, 스마트스토어 등에 공개된 전화번호는 해당 정보가 공개된 본래 목적(예: 상품 문의) 내에서만 이용이 가능합니다.
- 정보주체의 명시적 동의 없이 이를 크롤링하여 '선거운동'이라는 별개의 목적으로 사용하는 순간, 데이터 수집 행위 자체가 불법이 됩니다.

⚖ 이는 PIPA상 '목적 외 이용' 및 '무단 수집'에 해당하며, 이후의 모든 문자 발송 행위를 위법으로 오염시키는 근본 원인이 됩니다.

데이터 수집 단계의 리스크: 단순 과태료가 아닌 '형사 처벌' 대상

관련 법규 (Statute): 개인정보 보호법 (PIPA) 제71조 제1항 1호

위반 행위 (Violation): 정보주체의 동의를 받지 아니하고 개인정보를 수집하거나, 수집 목적의 범위를 초과하여 이용하는 행위.

법적 제재 (Penalty)

5년 이하의 징역 또는 5천만 원 이하의 벌금

문자메시지를 단 한 통도 보내지 않았더라도, 동의 없이 크롤링하여 연락처 목록을 생성하고 보유하는 것만으로도 중대한 형사 처벌 대상이 될 수 있습니다.
이는 선거법 위반과 별개로 적용되는 독립적인 범죄입니다.

제2단계 위법: 불법 데이터를 사용한 '선거 정보 전송'

불법적으로 수집된 데이터베이스를 사용하는 순간, 공직선거법(POEA)이 규정하는
모든 절차적 요건을 준수하더라도 전체 행위는 위법이 됩니다.
합법적인 선거운동은 합법적인 데이터 위에서만 가능합니다.

Key Areas of POEA Violation:

- 발송 주체의 자격 (Sender Eligibility)
- 전송 횟수 및 방법 (Frequency and Method)
- 발신 번호 신고 의무 (Registered Number Requirement)
- 필수 기재사항 명시 (Required Disclosures)

공직선거법(POEA)상 자동 동보통신 필수 준수사항 체크리스트

준수 항목 (Requirement)	POEA 규정 (Rule)	위반 사례 (Common Violation)	제재 (Penalty)
발송 주체 (Sender)	**후보자/예비후보자**에 한정 (20인 초과 동시 전송 시)	일반 선거운동원, 입후보 예정자가 자동 동보통신 사용	**형사 처벌 가능**
발송 횟수 (Frequency)	**총 8회 이내** (예비후보자+후보자 기간 포함)	8회를 초과하여 발송	**형사 처벌 가능**
발신 번호 (Sender ID)	선관위에 **신고한 1개의 번호만 사용**	미신고 번호 또는 개인 휴대폰 번호 사용	**1천만 원 이하 과태료**
필수 기재사항 (Disclosures)	(선거운동정보) 표시, **무료 수신거부(080) 방법 명시**	수신거부 안내 누락 또는 유료 번호 안내	**과태료 또는 형사 처벌**

최종 리스크 분석: '책임 중첩'의 완전한 그림

STARTING ACTION:
'크롤링 번호로 선거 문자 발송'

VIOLATION 1: 개인정보 보호법 (PIPA)

근거:
동의 없는 수집 및 목적 외 이용 (제71조)

책임:
형사 책임 (Criminal)

최대 5년 징역 / 5천만 원 벌금

VIOLATION 2: 공직선거법 (POEA)

근거:
미신고 번호 사용, 주체/횟수/기재사항 위반

책임:
행정 책임 (Admin) + **형사 책임** (Criminal)

최대 1천만 원 과태료 + 별도 형사 처벌

VIOLATION 3: 정보통신망법 (ICNA)

근거:
수신거부 회피 기술적 조치 등 (제50조)

책임:
형사 책임 (Criminal)

최대 1년 징역 / 1천만 원 벌금

ADDITIONAL RISK: 민사 책임 (CIVIL)

근거:
개인정보 침해에 따른 손해배상

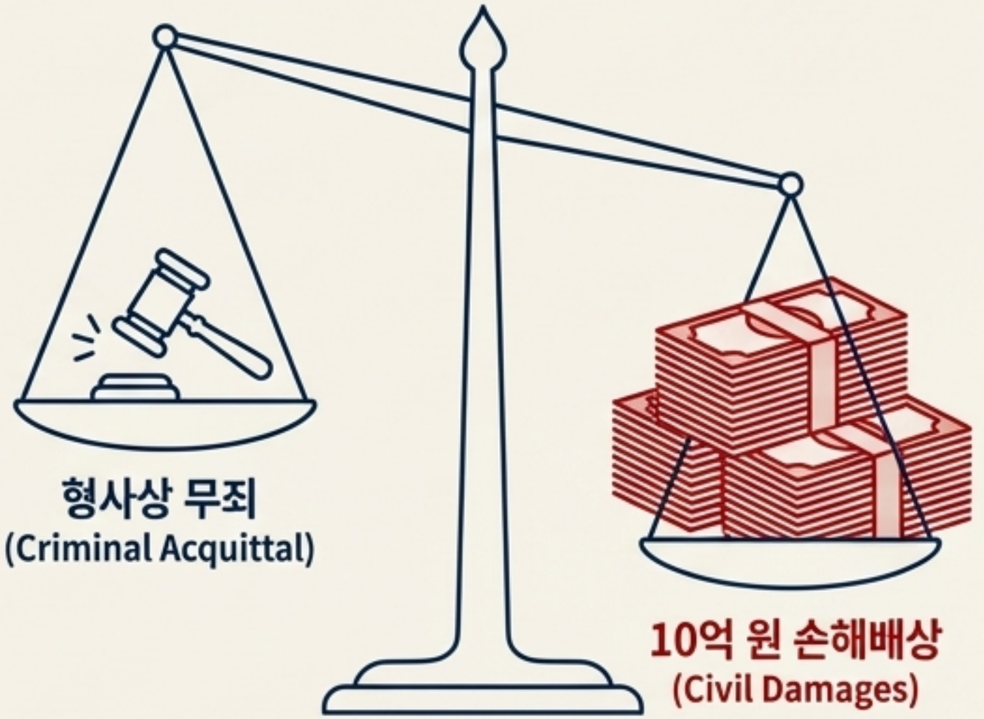
책임:
재정적 책임 (Financial)

거액의 집단 손해배상 소송 가능

형사 처벌을 피하더라도 남는 가장 큰 위험: '민사 집단소송'

'판례 핵심'

데이터 크롤링 관련 판례에서, 법원은 행위자에게 형사상 무죄를 선고했음에도 불구하고, 정보주체의 권리 침해를 인정하여 **민사적으로 10억 원에 달하는 손해배상을 명령**한 사례가 존재합니다.



캠페인에 미치는 치명적 영향

기하급수적 리스크
수천, 수만 명의 유권자로부터 개인정보 침해를 이유로 하는 집단 소송에 직면할 수 있습니다.

재정적 파탄
단 한 번의 불법 데이터 사용이 캠페인의 재정 기반 자체를 무너뜨릴 수 있는 절대적 리스크입니다.

평판 손상
법적 공방 과정에서 후보자와 캠페인의 도덕성에 치명적인 타격을 입게 됩니다.

사법부와 선관위의 엄격한 법 집행 기조

법원의 광범위한 해석
(Broad Interpretation by Courts)

판례

대법원은 스마트폰에 대량 발송 프로그램을 설치한 행위도 '컴퓨터를 이용한 자동송신장치'로 인정. 기술적 형태를 불문하고 대량·자동 전송 행위를 엄격히 규제합니다.

책임은 후보자에게 귀속
(Liability Attributed to the Candidate)

판례

선거사무장이 예비후보자의 지시에 따라 불법 문자를 보낸 경우, 이를 '예비후보자가 한 선거운동'으로 판단. 실무자의 행위가 후보자 본인의 형사 책임으로 이어질 수 있습니다.

선관위의 적극적인 고발
(Proactive Prosecution by NEC)

사례

대한약사회 선거에서 개인정보를 불법 수집하여 비방 문자를 보낸 행위자를 선관위가 직접 경찰에 고발. 데이터 수집의 불법성을 중대한 선거 범죄로 간주합니다.

흔한 오해 바로잡기: '(광고)' 문구만 넣으면 합법일까?

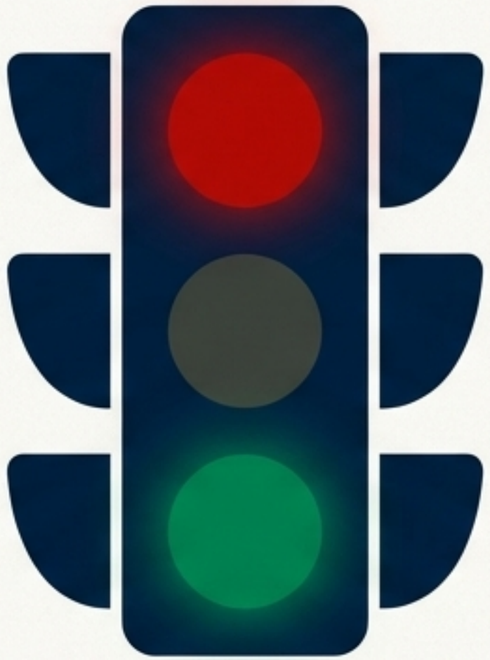
아닙니다. 법적 효력이 전혀 없습니다.

- **정보통신망법:** '(광고)' 표시는 필수 요건 중 하나일 뿐, **수신자의 '사전 동의'**라는 대전제를 대체할 수 없습니다.
- **개인정보 보호법:** 사전 동의 없이 연락처를 수집한 행위 자체가 이미 위법이므로, 이후 메시지 형식은 위법성을 해소하지 못합니다.

결론: 동의 없는 발송은 어떠한 형식을 취하더라도 불법입니다.

그렇다면 어떻게 해야 하는가: 법적 리스크 회피를 위한 캠페인 행동 강령

법적 리스크를 피하는 길은 복잡하지 않습니다. 데이터 획득부터 전송까지 전 과정에 걸쳐 명확한 원칙을 수립하고 준수하는 것이 핵심입니다. 다음 슬라이드는 캠페인 실무진이 반드시 숙지해야 할 'Red Flags'와 'Green Lights'입니다.



선거운동 문자 발송: 이것만은 반드시 지키십시오

RED FLAGS: 절대 금지

- **출처 불명의 데이터베이스:** 크롤링, 구매, 단순 교환 등 합법적 동의 절차를 입증할 수 없는 모든 연락처 목록.
- **'공개 정보'의 임의 사용:** 인터넷, 소셜미디어, 명함 등에 공개된 번호를 동의 없이 선거운동 DB에 추가하는 행위.
- **동의 기록 부재:** '언제, 어떤 경로로, 어떤 목적에' 동의했는지 입증할 기록이 없는 데이터.

GREEN LIGHTS: 필수 준수

- **명시적 동의 확보 및 기록:** 선거운동 정보 수신에 대한 정보주체의 명시적 동의를 받고, 그 증빙자료(서면, 녹취 등)를 철저히 보관.
- **POEA 절차 100% 준수:** 선관위 신고 번호 사용, 8회 횟수 제한, (선거운동정보) 및 무료수신거부(080) 번호 등 필수사항 명시.
- **정기적인 법률 자문 및 교육:** 캠페인 실무진을 대상으로 개인정보 및 선거법 관련 정기 교육을 실시하고, 중요 사안은 반드시 법률 자문을 거침.

데이터의 합법성이 선거운동의 성패를 좌우합니다

불법 크롤링을 통한 선거 문자는 단기적인 홍보 효과보다
법적, 재정적, 정치적 실패라는 훨씬 큰 대가를 치르게 합니다.

유권자의 개인정보를 존중하는 것은 법률 준수를 넘어, 신뢰를 기반으로 하는
선거운동의 가장 기본적인 원칙입니다.

가장 안전하고 효과적인 선거운동은 합법적으로 확보된 데이터에서 시작됩니다.